Data Protection Policy

This policy document is compliant with the provisions of the EU General Data Protection Regulation 679/2016.

This policy document sets out the policies and procedures CODESCREEN BRAINCUB INCUBATOR LTD will comply when dealing with personal data.

Personal data must be protected in accordance with the provisions of the General Data Protection Regulation 679/2016. Dependence on personal data for the normal conduct of business necessitates the creation of this policy to set out the procedures and measures to protect personal data.

This policy defines rules, procedures, and measures to collect, use, and store personal data in a GDPR-compliant manner and control and prevent unauthorized access to personal data. A breach of data security can lead to regulatory fines, an inability to provide services, loss of customer confidence, physical, financial and emotional damage to the affected persons.

This policy therefore discusses:

- Data categories
- Data classification
- Data ownership
- Data collection/generation
- Data usage
- Data storage
- Data disposal
- Data transfer
- Data security

This policy defines the CODESCREEN BRAINCUB INCUBATOR LTD overall data protection objectives and procedures that we endorse.

This embodies the principles of data protection as described in Article 5 of the GDPR, namely:

- Lawfulness, fairness and transparency,
- Purpose limitation,
- Data minimisation,
- Accuracy,
- Storage Limitation,
- Integrity and confidentiality

Breach of the policy and its consequences

A breach of this policy could have severe consequences to CODESCREEN BRAINCUB INCUBATOR LTD, its ability to provide services or maintain the integrity, confidentiality, or availability of services.

Intentional misuse of data resulting in a breach of any part of this policy will result in disciplinary action at the discretion of the senior management of CODESCREEN BRAINCUB INCUBATOR LTD. Severe, deliberate or repeated breaches of the policy by any employee may be considered grounds for instant dismissal, or in the case of a CODESCREEN BRAINCUB INCUBATOR LTD vendor, termination of their

contracted services. All employees and vendors are bound by these policies and are responsible for their strict enforcement.

Scope of the Policy

This policy applies to all CODESCREEN BRAINCUB INCUBATOR LTD and customer data assets that exist in any processing environment of CODESCREEN BRAINCUB INCUBATOR LTD, on any media during any part if its life cycle. The following entities or users are covered by this policy:Full or part-time employees of CODESCREEN BRAINCUB INCUBATOR LTD who have access to CODESCREEN BRAINCUB INCUBATOR LTD's or customer data.

This document forms part of ourconditions of employment for employees , contractual agreements for vendors, suppliers, and third party processor or agents, hereafter referred to as vendors. . All parties must read this policy completely, and confirm that they understand the contents of the policy and agree to abide by it.

Data Life Cycle

The security of data can be understood through the use of a data life cycle. The typical life cycle of data is collection/generation, use, storage and disposal. The following sections provide guidance as to the application of this policy through the different life cycle phases of data.

Users of data assets are personally responsible for complying with this policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data must only be used in a manner consistent with this policy.

Data Protection Policy Statement

Goals

This policy has been written with the following goals in mind:

- To ensure the security integrity and availability of all the company and customer data
- To establish the company baseline data security stance and classification schema
- that it should enable the firm to meet its own requirements for the management of personal information
- that it should support organisational objectives and obligations
- that it should impose controls in line with the firm’s acceptable level of risk;
- that it should ensure that the firm meets applicable statutory regulatory contractual and/or professional duties;
- that it should protect the interests of individuals and other key stakeholders

Processing environment

CODESCREEN BRAINCUB INCUBATOR LTD's processing environment that this policy applies to is comprised of:

- **Systems**– A system is an assembly of computer hardware (e.g. sub-networks application servers file servers workstations data etc.) and application software configured for the purpose of processing handling storing transmitting and receiving data which is used in a production or support environment to sustain specific applications and business organizations in their performance of tasks and business

processes.

- **Applications** – Application software is system or network-level routines and programs designed by (and for) system users and customers. It supports specific business-oriented processes jobs or functions. It can be general in nature or specifically tailored to a single or limited number of functions.
- **Networks** – A network is defined as two or more systems connected by a communication medium. It includes all elements (e.g. routers switches bridges hubs servers firewalls controllers and other devices) that are used to transport information between systems.
- **Mobile apps** – A mobile application most commonly referred to as an app is a type of application software designed to run on a mobile device such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs.

3. **Data Protection Responsibilities**

The Data Protection Office Department department is responsible for:

- Defining the security requirements controls and mechanism
- Defining the methods and guidelines used to identify and classify all data assets
- Defining the procedures for identifying data owners for all data assets
- Defining the labeling requirements for all data assets
- Defining procedures for data usage processing transmission storage and disposal
- Defining the procedures necessary to ensure compliance to this policy
- Facilitating the evaluation of new regulatory requirements and best practices

4. **Management Responsibilities**

Other departments within CODESCREEN BRAINCUB INCUBATOR LTD also have various responsibilities for ensuring compliance with this policy, such as:

- All individuals in the department must ensure that staff complies with this policy.
- The Data Protection Office Departmentmust ensure that adequate logs and audit trails are kept of all data access.
- The Data Protection Office Departmentmust ensure the activation of all security mechanisms.
- The Data Protection Office Department is responsible for communicating business requirements and issues for business processes and the data those include to ensure their correct data classification.
- The Data Protection Office Department is responsible for regularly evaluating the data classification schema for consistent application and use.

5. **Other Responsibilities**

Other departments and related entities have responsibilities to comply with this policy, such as:

All CODESCREEN BRAINCUB INCUBATOR LTD agents, vendors, content providers, and third party providers that process customer data must have a documented data protection policy that clearly identifies those data and other resources and the controls that are being imposed upon them.

All CODESCREEN BRAINCUB INCUBATOR LTD agents, vendors, content providers, and third party providers that access the CODESCREEN BRAINCUB INCUBATOR LTD processing environment and its data or provide content to it must have a security policy that complies with and does not contradict the CODESCREEN BRAINCUB INCUBATOR LTD data protection policy.

All agents, vendors, content providers, and third party providers must agree not to bypass any of our security requirements.

Data Classification

Data classification is necessary to enable the allocation of resources to the protection of data assets, as well as determining the potential loss or damage from the corruption, loss or disclosure of data.

To ensure the security and integrity of all data, the default classification for all data not classified by its owner must be Private Data

The Data Protection Office Department is responsible for the classification of data.

The Data Protection Office Department is responsible for evaluating the data classification schema and reconciling it with new data types as they enter usage. It may be necessary, as we enter new business endeavours, to develop additional data classifications.

All data found in the processing environment must fall into one of the following categorie(s):**Public Company Data** – Public company data is defined as data that any entity either internal or external to CODESCREEN BRAINCUB INCUBATOR LTD can access. The disclosure, use or destruction of Public company data will have limited or no adverse effects on CODESCREEN BRAINCUB INCUBATOR LTD nor carry any significant liability. (Examples of Public company data include readily available news, stock quotes, or sporting information.)

Data Ownership

In order to classify data, it is necessary that an owner be identified for all data assets. The owner of the data is DPO ZIRAVIX.

The owner of data is responsible for classifying their data according to the classification schema noted in this policy.

The Data Protection Office Department is responsible for developing, implementing, and maintaining procedures for identifying all data assets and associated owners.

Data collection/generation

Data will be collected in accordance with Article 13 and 14 of the GDPR, confirming to the transparency principle and ensuring that the data protection principles are duly observed.

Data may be collected in the following ways:Data gathered as a result of contracts between vendors and CODESCREEN BRAINCUB INCUBATOR LTD.

Each mode of data collection should have a specific purpose accompanied by one or more of the legal bases as defined in the GDPR.

Data Usage

All users that access CODESCREEN BRAINCUB INCUBATOR LTD or customer data for use must do so only in conformance to this policy. Uniquely identified, authenticated and authorized users must only access and use data.

Data should be used only for the stated purpose of its collection or generation. Any purpose outside the defined scope will be considered “misuse of data” and will entail consequences for the involved parties.

Each user must ensure that CODESCREEN BRAINCUB INCUBATOR LTD data assets under their direction or control are properly labelled and safeguarded according to their sensitivity, proprietary nature, and criticality.

Access control mechanisms must also be utilised to ensure that only authorized users can access data to which they have been granted explicit access rights.

Data Storage

The general premise for the data storage period is:

- for a time period necessary to fulfil that purpose.
- until the data subject submits a request to delete his/her data on justified grounds

All users that are responsible for the secure storage of CODESCREEN BRAINCUB INCUBATOR LTD or customer data must do so only in accordance with this policy.

Where necessary, data stored must be secured with encryption. This may include the use of confidentiality and/or integrity mechanisms. Specific cryptographic mechanisms are noted in the information security policy of CODESCREEN BRAINCUB INCUBATOR LTD.

Access control mechanisms must also be utilised to ensure that only authorised users can access data to which they have been granted explicit access rights.

Data Transmission

All users that access CODESCREEN BRAINCUB INCUBATOR LTD or customer data to enable its transmission must do so only in accordance with this policy.

Where necessary, data transmitted must be secured with encryption. This may include the use of confidentiality and/or integrity mechanisms. Specific cryptographic mechanisms are noted in the information security policy of CODESCREEN BRAINCUB INCUBATOR LTD.

The media used to distribute data should be classified so that it can be identified as confidential, and if the media is sent using a courier or other delivery methods, it should be accurately tracked.

No data can be distributed in any media from a secured area without proper management approval.

Data Disposal

The Data Protection Office Department must develop and implement procedures to ensure the proper disposal of various types of data. These procedures must be made available to all users with access to data that requires special disposal techniques.

Data should be disposed of in a secure manner so that it is completely destroyed and no information can be obtained from the waste.

- For electronic data the process of deletion will be carried out by electronic shredding.
- For paper records physical paper shredders will be used.
- All digital storage devices i.e. hard drives or flash drives will be completely destroyed so that no data is recoverable from them.

Policy Review

It is the responsibility of the Data Protection Office Department to facilitate the review of this policy on a regular basis. This policy will be reviewed Annually. Senior management, I.T and Systems administration,

Legal department should, at a minimum, be included in the Annually review of this policy.

Last updated: 2026-07-09