

Data Consent Policy

Introduction

This document sets out CODESCREEN BRAINCUB INCUBATOR LTD Data Consent Policy. It covers the processing and sharing of personal data. If you require advice and assistance around any data protection matter please contact CODESCREEN BRAINCUB INCUBATOR LTD Data Protection Officer

The GDPR and Consent

The GDPR sets a high standard for consent. Consent means offering individuals the power to choose and take control of their data.

Genuine consent will put individuals in charge, build customer trust and engagement, and enhance CODESCREEN BRAINCUB INCUBATOR LTD's reputation.

The GDPR states that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in).

It specifically bans pre-ticked opt-in boxes. It also requires an individual, also known as “granular” consent options for distinct processing operations. Consent is kept separate from other terms and conditions and should not be a precondition of signing up for a service.

The GDPR gives a specific right to withdraw consent. CODESCREEN BRAINCUB INCUBATOR LTD will inform individuals about their right to withdraw and offer easy ways for customers to withdraw consent at any time.

CODESCREEN BRAINCUB INCUBATOR LTD will keep clear records to demonstrate consent and regularly review existing consents and consent mechanisms that we rely upon to ensure they meet the GDPR standards.

Employees of CODESCREEN BRAINCUB INCUBATOR LTD must have respect for privacy and people's right to determine what happens to their personal and sensitive information.

If there is any doubt, contact the Data Protection Officer

CODESCREEN BRAINCUB INCUBATOR LTD and its employees and third-party providers have been trained, appraised and understand that:

- Individuals have the right to withdraw/withhold consent in most circumstances, and this right must be respected and recorded appropriately.
- Consent must be freely given, specific and informed.
- All employees must ensure they consider the safety and welfare of the individual when making decisions on whether to share information about them.
- All employees must establish the capacity of the individual's ability to provide consent.
- When requesting consent, staff must ensure that information is provided in a suitable, accessible format or language. If necessary, provide large print or Braille versions, accredited interpreters, signers, or other appropriate special communication skills.

Employees must record the decision to share personal information on an appropriate register or specific system which can be readily accessed in line with CODESCREEN BRAINCUB INCUBATOR LTD policies

and procedures on data protection.

What if there is no consent?

CODESCREEN BRAINCUB INCUBATOR LTD acknowledges that obtaining consent is not always possible, or consent may be refused. However, not obtaining consent or the refusal to give consent may not constitute a reason for not processing or sharing information.

There are certain situations where an individual's information can be disclosed without obtaining it.

Consent, if there is a lawful basis for processing without consent in place.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply. Whenever you process personal data without consent:

- a. Contract: the processing is necessary for a contract you have with the individual or because they have asked you to take specific steps before entering into a contract.
- b. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- c. Vital interests: the processing is necessary to protect someone's life.
- d. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- e. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Different criteria apply to sensitive personal information (now called "special categories of personal data"). This is now defined as data relating to:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

In order to process special category data legally, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.

In summary, these are:

- a. explicit consent of the person concerned
- b. for the purpose of carrying out the obligations, exercising specific rights of the controller or of the data subject in the field of employment and social security, and social protection
- c. to protect the vital interests of the data subject or of another natural person
- d. processing is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- e. the processing relates to personal data, which are manifestly made public by the data subject

- f. processing is necessary for the establishment, exercise or defence of legal claims
- g. processing is necessary for reasons of substantial public interest
- h. for the purpose of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment
- i. for reasons of public health
- j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Special Cases

Children

The duty of confidentiality owed to a child/young person who lacks capacity is the same as that owed to any other person. Occasionally, children/young people will lack the capacity to consent. An explicit request by a child that information should not be disclosed to parents or guardians, or indeed any third party, must be respected except where it puts the child at risk of significant harm, in which case disclosure may take place in the 'public interest' without consent.

Criminal Offences

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, criminal proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences or related security measures set out in Article 10 of the GDPR.

To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 of the GDPR and either legal authority or official authority for the processing under Article 10.

Article 10 also specifies that you can only keep a comprehensive register of criminal convictions if you are doing so under the control of the official authority.

If you are in any doubt as to how to go about handling special categories of data, such as data concerning children, sensitive data such as race and sexuality, or criminal data, see the checklist at the end of this policy statement and consult CODESCREEN BRAINCUB INCUBATOR LTD 's Data Protection Officer for further advice and guidance

Policy Breach Statement

Any breach of this Policy will be investigated and may result in disciplinary action. Serious breaches may be considered gross misconduct and result in dismissal without notice or legal action being taken against you. CODESCREEN BRAINCUB INCUBATOR LTD, as well as those individuals affected, is also at risk of financial and reputational harm. Fines of up to €20 million may be imposed on organisations for serious data breaches.

Please report any actual or potential data breaches or other concerns relating to Data Protection or consent to CODESCREEN BRAINCUB INCUBATOR LTD Data Protection Officer as soon as possible, in accordance with CODESCREEN BRAINCUB INCUBATOR LTD Data Breach Policy.

CHECKLIST

Asking for consent

- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes or any other type of default consent
- We use clear plain language that is easy to understand.
- We specify why we want the data and what we are going to do with it.
- We give individual granular options to consent separately to different purposes and types of processing.
- We name organisations and any third-party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent.
- We ensure that individuals can refuse to consent without detriment.
- We refrain making consent a precondition of a service
- If we offer online services directly to children we only seek consent if we have age verification measures and parental-consent measures for younger children in place.

Recording consent

- We maintain a record when and how we obtained consent from the individual.
- We maintain a record of exactly what they were told at the time

Managing consent

- We regularly review existing consent to check that the relationship the processing and the purposes have not changed.
- We have processes in place to refresh consent at appropriate intervals including any parental consents.
- We use privacy dashboard or other preference-management tools as a matter of good practice.
- We make it easy for individuals to withdraw their consent at any time and publicise how to do so.
- We act on withdrawals of consent as soon as we can.
- We do not penalise individuals who wish to withdraw consent.