Procedural Guide and Privacy Policy
Regarding Whistleblowing Reports

IDBC Creative Solutions Kft., IDBC New Tech Kft., and **IDBC GO Kft.** are engaged in providing human resources management and IT services related to business process management. Given that the target groups and business partners of the three companies are different, but the provision of services (searching for potential partners, contracting, fulfillment, etc.) mostly follows the same methodology, **the three companies have concluded a joint data controller agreement**.

The essence of the joint data controller agreement is that IDBC Creative Solutions Kft., IDBC New Tech Kft., and IDBC GO Kft. (hereinafter collectively: **IDBC** or **Data Controller**) jointly provide and operate the human resources and process management services belonging to their scope of activities (e.g., sales, customer relations). The preparation and updating of privacy policies, the handling of potential data breaches and reporting them to the data protection supervisory authority as necessary, as well as the exercising of data subject rights, are carried out with the cooperation of IDBC Creative Solutions Kft. If any data protection-related activity (e.g., modifying the privacy policy, contacting data subjects) affects the activities of IDBC New Tech Kft. and/or IDBC GO Kft., IDBC Creative Solutions Kft. acts after consulting with the Parties or the affected Party.

IDBC pays special attention to honest, supportive communication and cooperation that prioritizes solutions, while also considering reliability, accountability, and taking responsibility to be important. IDBC is committed to meeting present needs without compromising the ability of future generations to meet their own needs; therefore, alongside economic considerations, it also takes environmental and social factors into account during organizational operations and business decision-making.

In this Procedural Guide and Privacy Policy, we have summarized the information (procedure process, purpose, legal basis, and duration of data processing, the scope of processed personal data, etc.) concerning the procedural steps related to reporting abuses or suspected abuses arising during IDBC's business and employer activities, handling whistleblowing reports (receiving, evaluating, etc.), and the data processing necessary for this.

Legislation related to the processing and protection of personal data refers to:

a) the subject of the personal data (e.g., the natural person making the whistleblowing report) as the data subject (hereinafter: data subject),
b) any information relating to the data subject as personal data,
c) any operation performed on personal data (collection, recording, storage, processing, consultation, transmission, retrieval, viewing, disclosure, etc.) as data processing,
d) the authorization for data processing as the legal basis of data processing,
e) the decision-maker regarding the purposes and means of data processing as the data controller,
f) those who do not belong to the data controller but participate in data processing operations based on a written agreement as data processors,
g) a person other than the data subject, the data controller, and the data processor as a third party;

therefore, we use these terms in the Privacy Policy.

This Procedural Guide and Privacy Policy also contains the data protection, legal enforcement, and remedy rights of natural persons (see Section 8).

1. Names and Contact Details of Data Controllers

Data Controller 1: **IDBC Creative Solutions Kft.**

Headquarters and postal address: 1138 Budapest, Népfürdő u. 22. Duna Tower Irodaház A torony 13. emelet

Registering authority: Company Registry Court of the Budapest Metropolitan Court

Company registration number: 01-09-192925

Tax number: 24983332-2-41

Recruitment agency license number: BPM/0701/597-1/2016-1012

E-mail address: info@idbc.hu

Phone number: +36 30 479 8090

Website: https://idbc.hu

Data Protection Officer contact: adatvedelem@idbc.hu

Data Controller 2: **IDBC New Tech Kft.**

Headquarters and postal address: 1138 Budapest, Népfürdő u. 22. Duna Tower Irodaház A torony 13. emelet

Registering authority: Company Registry Court of the Budapest Metropolitan Court

Company registration number: 01-09-861417

Tax number: 13556075-2-41

E-mail address: info@idbc.hu

Phone number: +36 30 479 8090

Data Protection Officer contact: adatvedelem@idbc.hu

Data Controller 3: **IDBC GO Kft.**

Headquarters and postal address: 1138 Budapest, Népfürdő u. 22. Duna Tower Irodaház A torony 13. emelet

Registering authority: Company Registry Court of the Budapest Metropolitan Court

Company registration number: 01-09-283268

Tax number: 25578182-2-41

E-mail address: info@idbc.hu

Phone number: +36 30 479 8090

Data Protection Officer contact: adatvedelem@idbc.hu

2. Important Legislation Regarding Data Processing

a) Regulation (EU) 2016/679 of the European Parliament and of the Council (April 27, 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR or General Data Protection Regulation)
b) Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Info Act)
c) Act V of 2013 on the Civil Code (Civil Code)
d) Act XXV of 2023 on complaints, public interest disclosures, and rules related to reporting abuses (Whistleblowing Act)

3. Procedural Guide

A whistleblowing report can be made in the event of acts or suspected acts violating the rules specified in Annex I of the Whistleblowing Act (market abuse, money laundering, and terrorist financing) or the rules and values written in IDBC's Code of Ethics (link).

Whistleblowing reports are handled by an impartial employee of IDBC designated to receive and investigate reports. The investigation of a whistleblowing report is aimed at determining what action (e.g., requesting further information, hearing the reporting person and/or the person concerned in the report, forwarding the report to another competent body) is necessary based on the content of the report.

A whistleblowing report can be made with a name or anonymously. IDBC may omit the investigation of reports that do not contain sufficient information to investigate the abuse if there is no way to obtain the further data necessary to conduct the procedure.

If the report comes from a sender who can be contacted, the reporting person will receive an acknowledgment of the receipt of the whistleblowing report within a maximum of seven days. The investigation of the whistleblowing report lasts for up to 30 days from receipt, which in justified cases – with simultaneous notification of the reporting person maintaining contact – can be extended by a maximum of another two months. The notification to the reporting person will include the expected deadline for the investigation of the whistleblowing report and the reasons for extending the deadline.

During the investigation of the whistleblowing report, the IDBC employee conducting the investigation keeps in touch with the reporting person who agrees to maintain contact and may request further information, clarification, or supplementation from them.

The IDBC employee conducting the investigation informs the reporting person who agrees to maintain contact in writing about the investigation of the report or its omission and the reason for the omission, the result of the investigation of the report, and the actions taken or planned.

For the operation of the internal whistleblowing channel receiving electronic messages, IDBC uses the services of FaceUp (further details about FaceUp can be found in Section 6).

During the investigation of whistleblowing reports and the remedying of the reported act, IDBC processes only the most necessary personal data, confidentially, for a specified period. The person designated to investigate the report promptly deletes personal data included in the whistleblowing report that cannot be directly linked to the abuse or its remedy.

The reported person may exercise their data subject rights related to the processing of personal data while ensuring the protection of the reporting person's personal data (i.e., the reported person cannot learn the personal data of the reporting person).

4. Activities Involving the Processing of Personal Data

4.1. Handling Whistleblowing Reports Based on the Whistleblowing Act

The legal basis for processing personal data included in a whistleblowing report containing an act according to Annex I of the Whistleblowing Act is the performance of a legal obligation under Section 17 and Section 18 (1) of the Whistleblowing Act, based on GDPR Article 6 (1) point c).

Scope of processed personal data:

a) the name and e-mail address of the reporting person, and other information provided in the report (e.g., job role, place, time, and description of the reported event),
b) the name of the reported person, and other information regarding the reported person provided in the report or arising during the investigation of the whistleblowing report (e.g., job role, place, time, and description of the reported event),

c) the name of a person having information regarding the reported event and other information related to them provided in the report or arising during the investigation of the whistleblowing report (e.g., job role, place, time, and description of the reported event).

If the report also contains personal data belonging to special categories of personal data, IDBC processes them based on the exception under GDPR Article 9 (2) point f) (processing is necessary for the establishment, exercise, or defense of legal claims).

Retention period of personal data: 5 years from the last action (closure) of the investigation of the whistleblowing report (general limitation period).

If the whistleblowing report results in an official or court procedure, the retention of personal data lasts until the retention period of the data of the official or court procedure.

4.2. Handling Whistleblowing Reports Regarding Violations of IDBC's Code of Ethics

The legal basis for processing personal data included in a whistleblowing report containing an act violating the value or values under IDBC's Code of Ethics is IDBC's legitimate interest in lawful, fair, and transparent operation, maintaining a good reputation, ensuring equal treatment, respecting human rights, and ensuring proper and safe operation (including the protection of trade secrets, corporate assets, and personal data), based on GDPR Article 6 (1) point f).

Scope of processed personal data:

a) the name and e-mail address of the reporting person, and other information provided in the report (e.g., job role, place, time, and description of the reported event),
b) the name of the reported person, and other information regarding the reported person provided in the report or arising during the investigation of the whistleblowing report (e.g., job role, place, time, and description of the reported event),
c) the name of a person having information regarding the reported event and other information related to them provided in the report or arising during the investigation of the whistleblowing report (e.g., job role, place, time, and description of the reported event).

If the report also contains personal data belonging to special categories of personal data, IDBC processes them based on the exception under GDPR Article 9 (2) point f) (processing is necessary for the establishment, exercise, or defense of legal claims).

Retention period of personal data: 5 years from the last action (closure) of the investigation of the whistleblowing report (general limitation period).

5. Profiling, Automated Decision-Making

IDBC does not apply profiling (grouping, evaluation according to a certain characteristic, etc.) using the personal data processed in connection with whistleblowing reports, nor does it apply automated decision-making based on this (a decision made exclusively by automated means affecting the data subject, or the computerized preparation of such a decision).

6. Access to Data, Data Transfer

Information related to whistleblowing reports is accessed by the person designated to receive and investigate whistleblowing reports. If absolutely necessary for the investigation of the whistleblowing report, data transfer may occur while ensuring the protection of personal data (e.g., requesting information to support the facts, based on the data subject's consent, data transfer due to competence).

For the operation of the internal whistleblowing system, IDBC uses the services of FaceUp Technology s.r.o. (Headquarters: Jiráskova 222/18, 602 00 Brno – střed; website: https://www.faceup.com/en, privacy policy: https://www.faceup.com/en/privacy-policy).

FaceUp qualifies as a data processor, which cannot make decisions related to data processing (e.g., for what purpose, what personal data to process, for how long); it is exclusively entitled to act and perform specified data processing operations (e.g., collection, analysis, transmission, erasure) according to the data processing agreement (FaceUp's data processing terms are available here: https://www.faceup.com/en/data-processing-addendum) and the instructions received.

IDBC may occasionally transfer personal data to the National Authority for Data Protection and Freedom of Information, which performs data protection supervision, or to other authorities or courts for their proceedings.

7. Data Security

IDBC ensures through IT, organizational, and personnel measures that the personal data it processes is protected against, among other things, unauthorized access, unauthorized alteration, or destruction.

Access to personal data processed in the internal whistleblowing system is role-based and logged. Authorized, trained employees of IDBC can access the processed personal data exclusively to perform their job tasks and to the extent necessary for that purpose.

FaceUp applies numerous data security measures [e.g., encrypted data traffic, operation according to the ISO 27001 (information security management system) standard, regular and automated backups, strict password policy, employee training, regular testing of protection against unauthorized intrusion, incident management, etc.]. Further details about FaceUp's data protection and data security measures can be read at the previously referenced links.

8. Rights of the Data Subject Regarding Data Processing

8.1. Right of access by the data subject

The data subject may request information in writing from IDBC through the contact details provided in Section 1 about what personal data of theirs is being processed, on what legal basis, for what data processing purpose, from what source, for how long, and to whom, when, based on what legislation the Data Controller granted access to which of the data subject's personal data, or to whom it transferred them.

IDBC fulfills the data subject's request within a maximum of one month in a response letter sent to the contact address provided by the data subject.

If the data subject requests the information under this section in multiple copies, the Data Controller is entitled to charge a reasonable fee proportionate to the administrative costs of producing the additional copies.

If the data subject's right of access under this section adversely affects the rights and freedoms of others, in particular the trade secrets or intellectual property of others, IDBC is entitled to refuse the fulfillment of the data subject's request to the necessary and proportionate extent.

Prior to fulfilling the request, IDBC may ask the data subject to clarify the content of the request and exactly specify the requested information and data processing activities.

8.2. Right to Rectification

The data subject may request in writing, through the contact details provided in Section 1, that IDBC modify any of their personal data (for example, they can change their e-mail address or other contact details at any time) or supplement incomplete personal data.

The Data Controller fulfills the request within a maximum of one month, and notifies the data subject of this in a letter sent to the contact address they provided.

IDBC informs those to whom it transferred the data subject's personal data about the rectified data, provided that the information is not impossible or does not require a disproportionate effort from the Data Controller.

8.3. Right to Erasure

The data subject may request in writing from IDBC, through the contact details provided in Section 1, the erasure of all or some of their personal data. IDBC will not fulfill the erasure if legislation obliges the further storage of personal data, and the data processing deadline specified by legislation has not yet expired.

If there is no such obligation, IDBC processes the data subject's request within a maximum of one month and notifies the data subject of the result in a letter sent to the contact address they provided.

IDBC informs those to whom it previously transferred the data subject's personal data about the erasure of the data, provided that informing them is not impossible or does not require a disproportionate effort from the Data Controller.

8.4. Right to Blocking (Restriction of Data Processing)

The data subject may request in writing, through the contact details provided in Section 1, that IDBC block their personal data. Blocking is done by clearly indicating the restricted nature of the data processing and storing it separately from other data. This means that, with the exception of storage, no other data processing operation may be performed on the data. The blocking lasts as long as the reason indicated by the data subject necessitates the blocked storage of the personal data.

The data subject may request the blocking of personal data, for example, if they believe that IDBC has processed their personal data unlawfully, but it is necessary for the official or court procedure initiated by them that the Data Controller does not erase the personal data. In this case, IDBC processes the personal data in a blocked manner until requested by the authority or court, and erases or continues to process them after the conclusion of the official procedure.

8.5. Right to Object

The data subject may object in writing to the data processing through the contact details provided in Section 1 if it is necessary for data processing based on IDBC's legitimate interests, except where IDBC demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims.

IDBC investigates the data subject's objection within a maximum of one month, and notifies the data subject of the result (including the communication regarding the erasure of any unlawfully processed personal data) in a letter sent to the contact address they provided.

9. Enforcement and Remedy Options Related to Data Processing

In order to enforce their rights related to the processing and protection of their personal data, the data subject may contact IDBC through the contact details of the data controllers specified above.

If the data subject believes that their rights to the protection of their personal data have been violated, they can seek a legal remedy from the following authority:

National Authority for Data Protection and Freedom of Information (NAIH)

Headquarters: 1055 Budapest, Falk Miksa u. 9–11.

Postal address: 1363 Budapest, Pf. 9.

Phone: +36 (1) 391-1400

Website: About the Authority

E-mail: ugyfelszolgalat@naih.hu

If the data subject experiences the unlawfulness of the processing of their personal data, they can initiate a court procedure (civil lawsuit) against the Data Controller. The adjudication of the lawsuit falls under the jurisdiction of the regional court (törvényszék). At the choice of the data subject, the lawsuit can also be initiated before the regional court corresponding to the data subject's place of residence (you can view the contact details of the regional courts via the following link: https://birosag.hu/torvenyszekek).

10. Updating and Availability of the Privacy Policy

IDBC reserves the right to unilaterally modify this Procedural Guide and Privacy Policy.

The modification of the Procedural Guide and Privacy Policy may occur, in particular, if necessary due to changes in legislation, the practice of the data protection supervisory authority, business needs, or newly discovered security risks.