

Privacy Policy for Applicants to Human Resources Management Services

IDBC Creative Solutions Kft. and **IDBC New Tech Kft.** are engaged in finding, recruiting, selecting, and placing professionals (candidates) seeking or interested in employment or assignments, as well as presenting and delivering job or assignment opportunities to candidates, i.e., providing human resources management services. Given that the target groups and business partners of the two companies are different, but the provision of human resources management services mostly follows the same methodology, **the two companies have concluded a joint data controller agreement.**

The essence of the joint data controller agreement is that IDBC Creative Solutions Kft. and IDBC New Tech Kft. (hereinafter collectively: **IDBC** or **Data Controller**) jointly provide and operate the human resources management service (recruitment) and its operation (sales, customer relations, employment, database). The preparation and updating of the privacy policy, 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., IDBC Creative Solutions Kft. acts as agreed upon with IDBC New Tech Kft.

The protection of your personal data is important to us, therefore in this Privacy Policy, we explain what personal data IDBC processes during recruitment, selection, and placement, for what purpose and legal basis, and what organizational and technical measures it takes to comply with data protection rules.

Data protection legislation refers to natural persons as "data subjects," therefore, in addition to or instead of "candidate," we also use this term in the Privacy Policy.

Further useful concepts related to the processing and protection of personal data included in the information below:

- a) personal data: any information relating to the data subject and which can be linked to them;
- b) data processing: any operation performed on personal data (collection, recording, storage, processing, consultation, transmission, retrieval, viewing, disclosure, etc.);
- c) data controller: the decision-maker regarding the purposes and means of data processing;
- d) data processor: those who do not belong to the data controller but participate in data processing operations based on a written agreement;
- e) third party: a person other than the data subject, the data controller, and the data processor (e.g., a job advertisement intermediary).

Becoming acquainted with this Privacy Policy is a condition for using IDBC's human resources management services, whether the candidate contacts IDBC directly or through an intermediary (job advertiser, recruitment agency, or recommendation by a natural person).

Legal entities that are job advertisers or recruitment agencies qualify as data controllers, and IDBC considers their personal data processing to be lawful and compliant with data protection legislation, meaning they make all information related to data processing (including data transfer) available to the candidate. For further details on the use of intermediaries, see Section 3.2.

Regarding personal data received through/upon the recommendation of a natural person (e.g., CV, LinkedIn profile), **IDBC assumes that the candidate is aware of the recommendation to IDBC and that they became acquainted with this Privacy Policy before their application data** (e.g., CV, professional information, contact details) was handed over to the recommender.

The Privacy Policy also contains the data protection rights of natural persons.

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

Company registration number: 01-09-192925

Registering authority: Company Registry Court of the Budapest Metropolitan Court

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

Tax number: 24983332-2-41

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

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 I of 2012 on the Labor Code (Labor Code)
- d) Act V of 2013 on the Civil Code (Civil Code)

3. Activities Involving the Processing of Personal Data

3.1. Applying for Human Resources Management Service, Initiating Contact by the Candidate

If the candidate contacts IDBC on IDBC's website, on the subpage containing job advertisements, or through any published contact details of IDBC (e.g., LinkedIn), or in response to a job advertisement published by IDBC, and provides their personal data (e.g., name, e-mail address, CV), we consider that they have initiated the use of IDBC's human resources management services. IDBC keeps records of the information provided by candidates during contact.

Purpose of data processing: identification of the candidate, presentation of a job application or assignment opportunity to the candidate, keeping contact.

Scope of processed personal data: name, contact details (e-mail address, phone number), information provided in the CV (e.g., data on expertise, work experience), job search criteria, other information provided by the data subject (e.g., motivation letter).

Legal basis for data processing: GDPR Article 6 (1) point a) – the consent of the data subject, which they provide by applying for a job application or recruitment.

Duration of personal data processing: until the withdrawal of the data subject's consent.

3.2. [Contact for Human Resources Management Service, Initiated by IDBC](#)

Contact with the candidate may also be initiated by IDBC, and the job or assignment opportunity may arise at IDBC or at one of its business partners. The intermediary for the candidate's personal data (e.g., CV) can be a natural person (e.g., employee referral) or a legal entity (e.g., job portal). **IDBC considers** that the accessibility of the candidate's personal data (e.g., handing over their CV or uploading it to a job portal) means that they are also aware of their transmission, and therefore the data subject accepts contact by IDBC.

IDBC currently cooperates with the following legal entity intermediaries:

- a) **Profession.hu** (Headquarters: 1123 Budapest, Nagyenyed utca 8-14., company registration number: 01-09-199015, private recruitment agency registration number: BPM/01/15807-3/2015-1003), privacy policy: [GDPR Profession](#)
- b) **LinkedIn** (Headquarters: 1000 W Maude Sunnyvale, CA 94085, US), privacy policy: [LinkedIn Privacy Policy](#)

IDBC occasionally also receives personal data related to candidates from other recruitment agencies that cannot be predetermined due to their ad hoc nature.

During contact, IDBC provides information about the source from which it obtained the candidate's personal data (e.g., name, phone number).

Purpose of data processing: identification of the candidate, provision of human resources management services, presentation of a job application or assignment opportunity to the candidate, keeping contact.

Scope of processed personal data: name, contact details (e-mail address, phone number), information provided in the CV (e.g., data on expertise, work experience), job search criteria.

Legal basis for data processing: GDPR Article 6 (1) point f) – IDBC's legitimate interest in finding job applicants and conducting its human resources management activities.

Duration of personal data processing:

- a) until the data subject's consent to data processing is provided, in the absence thereof, 30 days from obtaining the data;
- b) if, during contact, the candidate indicates that they do not wish to use the human resources management service or do not wish to receive information from IDBC about job applications or assignment opportunities, 5 working days from the communication of the rejection of IDBC's services.

3.3. [Data Processing Related to the Selection Procedure](#)

Beyond the job interview, we classify as part of the selection procedure every activity that IDBC performs after the receipt of personal data and the initial contact with the candidate, and which occurs in the interest of placing the candidate (e.g., evaluating the candidate, weighing selection criteria, mediating the candidate). The selection procedure qualifies as a contract-like relationship between the candidate and IDBC.

Purpose of data processing: performance of human resources management services, processing of the candidate's personal data and criteria regarding the search for a job or assignment opportunity, finding and presenting a job or assignment opportunity, conducting a selection procedure (e.g., interview), transmitting personal data to the potential employer, keeping contact with the candidate.

Scope of processed personal data: the candidate's personal identification data (name, place and date of birth, mother's name), contact details (phone number, e-mail address, mailing address and/or home address), data on their expertise and work experience (educational qualifications, previous workplaces, job roles, etc.), criteria for a job or assignment opportunity (e.g., remote work, fixed-term assignment).

In addition to the data falling into the listed types, IDBC processes all personal data that the candidate makes available during the human resources management services (including e.g., recruitment and the selection procedure) (e.g., candidate's profile on a social media site, marital status, interests, content of a motivation letter, fact of becoming acquainted with the privacy policy).

Legal basis for data processing: GDPR Article 6 (1) point b) – performance of a contract.

Duration of personal data processing: 5 years from the termination of the contract (general limitation period under the Civil Code). The contract is also considered terminated if the candidate requests the erasure of their data from IDBC's database.

3.4. Data Processing Related to Exercising the Data Subject's Rights and Complaints Regarding Personal Data Processing

The data subject may exercise their rights set out in Chapter 8 during all data processing activities carried out by IDBC, and may file a complaint regarding the processing of their personal data with the Data Controller or exercise their right to legal remedy as described in Chapter 9. In the submission related to exercising the data subject right, it is recommended to provide the contact detail (e.g., e-mail address or notification address) where the data subject wishes to receive our response regarding the exercise of their right.

We will respond to a submission related to the exercise of a data subject right within a maximum of 30 days from receipt.

If the request to exercise a data subject right does not contain enough information to exercise the right or to identify the data subject, IDBC will request the missing information.

Data subject rights are personal rights that can only be exercised personally. The term "exercised personally" means that these rights can be exercised by the person to whom the personal data related to the exercise of the right or the data processing activity affected by the privacy complaint relates, therefore IDBC may request proof of identity from the person exercising the data subject right.

The full processing of the data subject's personal identification data (name, place and date of birth, mother's name) only takes place if the data subject right cannot be exercised without providing these data, or the complaint regarding data processing cannot be evaluated.

Information that IDBC can verify in its own records (e.g., e-mail address, phone number) is suitable for proving identity. Sending a copy of an ID document electronically or by mail is not suitable for identity verification; IDBC will return such mail to the sender or delete/destroy it. In the absence of sufficient personal data necessary for identification, we may ask the data subject questions to establish identity that only they could know the answer to.

If the data subject does not provide the information necessary to exercise data subject rights or does not provide it sufficiently (e.g., does not provide their name or other identifying data), we are

unable to ensure the exercise of the data subject right, and we will reject the fulfillment of the request.

If the exercise of the data subject right or the privacy complaint 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 or to give a restricted response.

Purpose of data processing: ensuring the exercise of data subject rights, handling privacy complaints (receiving, evaluating, etc.).

Scope of processed personal data: the data subject's personal identification data (name, place and date of birth, mother's name), contact details (e-mail address, phone number, home address/ mailing address), data related to the exercise of the data subject right (topic, time, data related to fulfillment).

Legal basis for data processing: GDPR Article 6 (1) point c) – fulfilling a legal obligation according to GDPR Article 12 (5) and (6), Articles 15–18, Article 21.

Duration of personal data processing: 5 years from the closure of the exercise of the data subject right (general limitation period).

If the exercise of the data subject's rights or the handling of the privacy complaint entails an official or court procedure, the duration of data processing under this section lasts until the retention period of the documents of the official or court procedure.

3.5. Enforcement of Legal Claims

IDBC may enforce its legal claims (e.g., damages) related to its human resources management services.

Purpose of data processing: enforcement of claims related to the performance of the contract.

Scope of processed personal data: name, contact details (e-mail address, phone number), information related to the legal claim (e.g., name, content, time of the claim).

Legal basis for data processing: GDPR Article 6 (1) point f) – IDBC's legitimate interest in enforcing legal claims related to the provision of its human resources management services.

Duration of personal data processing: 5 years from the final conclusion of the procedure for enforcing the legal claim (general limitation period).

4. Data Transfer

IDBC transfers the candidate's personal data exclusively **in accordance with prior consultation with the candidate**, to those who have a job or assignment opportunity of interest to the candidate, or who may find such an opportunity for the candidate.

Furthermore, IDBC only transfers the personal data it processes to a third party (e.g., authority, court, or other state body) for purposes and in manners specified by law.

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.

5. Profiling, Automated Decision-Making

From the personal data it processes, IDBC occasionally carries out profiling (grouping according to a certain characteristic) with the help of conclusions drawn from the candidate's educational qualifications, interests, and job role, which it uses to define the target audience of thematic newsletters.

IDBC does not apply automated decision-making (decisions made exclusively by automated means affecting the data subject) during profiling or based on it.

6. Data Processing

Data processors may not make decisions related to data processing (e.g., for what purpose, what personal data to process, for how long), they are exclusively entitled to act and perform specified data processing operations (e.g., collection, analysis, transmission, erasure) according to the contract concluded with IDBC and the instructions received. IDBC only uses data processors that implement appropriate technical and organizational measures in order to guarantee a level of data protection and data security corresponding to the degree of risk.

IDBC processes personal data relating to candidates electronically, for which it uses the **Zoho Recruit module** ([Hiring software | Automated hiring platform - Zoho Recruit](#)). Further details on Zoho's data protection and data security principles can be read here ([Zoho - Data Privacy and our stand against surveillance](#)), and its privacy policy here ([GDPR Guide | Free e-book - Zoho Recruit](#)).

With a business subscription, IDBC uses the **Microsoft 365** and Microsoft Teams services of Microsoft Ireland Operations Limited (Headquarters: Ireland, Dublin 18, Leopardstown, South County Business Park, One Microsoft Place, privacy policy: [Microsoft Privacy Statement - Microsoft Privacy Practices](#)).

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 stored in the IT system is role-based and logged, meaning it can always be verified who accessed what personal data and when. 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.

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 Data Portability](#)

The data subject may request in writing, through the contact details provided in Section 1, that IDBC provide their personal data processed in an automated manner based on the data subject's consent [GDPR Article 6 (1) point a)] or performance of a contract [GDPR Article 6 (1) point b)] in a structured, commonly used, machine-readable format.

If it is otherwise technically feasible, IDBC will, at the data subject's request, transmit the personal data directly to another data controller indicated in the data subject's request.

The right to data portability under this section does not create an obligation for data controllers to adopt or maintain processing systems or applications that are technically compatible with each other.

If the data subject's right to data portability 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 extent.

8.4. [Right to Withdraw Consent to Data Processing](#)

Through the contact details provided in Section 1, in the same manner as the consent to data processing was given (e.g., unsubscribing in the case of subscribing, removing a mark if a mark was placed), the data subject may withdraw their consent to data processing at any time, which does not affect the lawfulness of data processing before the withdrawal of consent.

The withdrawal of consent given for data processing results in the erasure of personal data.

8.5. [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.

8.6. [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.

8.7. [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 Privacy Policy.

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