PRIVACY POLICY FOR JOB APPLICATIONS

These information relate to the processing of personal data that Corvinus University of Budapest collects and processes about the applicants for published vacancies.

1. DATA CONTROLLER

Corvinus University of Budapest (hereinafter referred to as CORVINUS or University)
1.1. Unit: HR
Address:1093 Budapest, Fővám tér 8.
Website:https://www.uni-corvinus.hu/
E-mail: career[at]uni-corvinus[dot]hu

1.2. Data Protection Officer (DPO): Marica SÁRKÖZI-KEREZSI
E-mail: marica[dot]kerezsi[at]uni-corvinus[dot]hu

2. LEGISLATION UNDERLYING DATA PROCESSING

- REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 (General Data Protection Regulation);
- Act CXII of 2011 on informational self-determination and freedom of information (Privacy Act);
- Act CCIV of 2011 on national higher education (hereinafter: 'National Higher Education Act').

3. CATEGORIES OF DATA SUBJECTS

The data processing concerns applicants for jobs published by Corvinus University of Budapest.

4. SCOPE, LEGAL BASIS, PERIOD, SOURCE OF THE DATA PROCESSING

4.1. PURPOSE OF THE DATA PROCESSING CORVINUS processes the personal data specified in point 4.2 for the purpose of selecting the right employee for the job published, and to register the personal data provided in the application for recruitment and selection of the applicants for later job applications, based on their specific consent, and to contact any potential applicants directly.

4.2. THE SCOPE: Applicant's application files, the personal data provided therein, as well as the data necessary for assessing the suitability for the position, in particular CV, cover letter, identity data, data on school qualifications, current and previous employment/work relationship data, contact data. CORVINUS does not request personal data (e.g. interests, leisure activities, marital status, photograph) from the applicants if such data are provided in the relevant application file, and if not necessary for the assessment. Such the data are stored by CORVINUS as part of the application file or, if possible, shall return to the applicant.

4.3. LEGAL GROUNDS:
a) In respect of the applicant's personal data (e.g. name, place of birth, date of birth, mother's name) and the contact details provided (postal address, phone number, e-mail address), the data subject's consent [Art. 6 (1) (a) GDPR] by submitting the application in the light of the data processing information published on the website;
b) in respect of the data necessary for the assessment of suitability for the position (e.g. language examination certificate, professional experience) – legitimate interest [Art. 6 (1) f) GDPR] except for the legal basis set out in subpoint c);
c) in respect of the data required to certify the qualifications and professional qualifications specified in the recruitment notice, data processing is based on Section 24 (5) of the Nftv. - complience with a legal obligation [Art. 6 (1) c) GDPR].

4.4. PERIOD OF THE DATA PROCESSING:
a) in the case of voluntary consent as defined in point 4.3 a), until the withdrawal of the consent, but no later than 5 working days after the closing of the application procedure, whether successful or unsuccessful, or, in the case of the applicant's specific consent (marked checkbox), until the withdrawal of the consent, but no later than 31 December of the year after the submission of the application file;
b) in the case of a legitimate interest as defined in point 4.3 b), up to a maximum of 5 working days after closing the application procedure, whether successful or unsuccessful, or until the withdrawal of the call;
c) in the case of compliance with the legal obligation set out in point 4.3 c), up to a maximum of 5 working days after closing the application procedure, whether successful or unsuccessful, or until the withdrawal of the call.

4.5. SOURCES: CORVINUS does not process data that is not collected from the data subject during this data processing.

5. ACCESS TO DATA

The relevant employees and bodies of the organisational units involved in the implementation of the purposes of the data processing described in point 4, in order to carry out their duties, as specified in the university regulations, have access to personal data on behalf of CORVINUS. As specified in the university regulations, documents of certain bodies are public and published on the University's website in a way that is accessible to all university citizens, for example in the case of the Senate.

6. TRANSFERRING DATA

The University shall disclose data to third parties only on the basis of a legal authorisation or under the consent of the data subject. No personal data is transferred to third countries.

7. TECHNICAL SECURITY MEASURES

CORVINUS shall take appropriate technical and organisational measures to ensure that the personal data under its processing are protected against accidental or unlawful destruction, loss, alteration and unauthorized processing, access and disclosure.

8. ENGAGING OTHER PROCESSORS

In the course of this data processing, the University does not use other data processors.

10. RIGHTS RELATED TO DATA PROCESSING

10.1. Right to request information

The data subject may request information from the controller in writing via any contact provided in point 1.1 on:

- the nature of the processed personal data,
- the legal grounds of the data processing,
- the purposes of the data processing
- the sources,
- the duration of the data processing,
- to whom, when, under what laws, which personal data the University has granted access to, or to whom it has transferred your personal data.

10.2. *Right to rectification*

The data subject may request the controller in writing via any contact provided in point 1.1 to change any personal data (for example change of email address or postal address).

10.3. Right to erasure

The data subject may request the University in writing via any contact provided in point 1.1 to erase his or her personal data. No erasure may be requested if the data processing is prescribed by law.

10.4. Right to blocking (restriction of processing)

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

Blocking your personal data may be requested from the controller in writing (while clearly indicating the restricted nature of the data processing and ensuring that the processing is separated from other data) via any the contact details provided in point 1.1. The blocking shall continue for as long as the reasons indicated by the data subject so require.

10.5. Right to object

You may object to the processing of the data in writing with respect to your data provided in point 4.3 b) via the contact details provided in point 1.1. An objection is a statement in which you object to the processing of your personal data.

10.6. Right to withdrawal of consent

You may withdraw your consent in writing at any time with respect to your data provided in point 4.3 a) via the contact details provided in point 1.1, collectively or individually at your discretion. Such withdrawal of consent shall not affect the lawfulness of previous processing.

10.7. The data subject has *Right to data portability* in respect of data processed in an automated manner in accordance with point 4.3 a)) [Article 20 GDPR]

The controller shall provide information in writing, in an intelligible form, without undue delay but no later than within 1 month from the date of submission of the request, about the measures taken or the rejection of the request and its reasons.

11. LAW ENFORCEMENT RELATED TO DATA PROCESSING

In case of unlawful data processing, the National Authority of Data Protection and Freedom of Information (NAIH) or the court can be contacted as follows:

11.1. Official report

If you believe that there has been an infringement or imminent threat of an infringement of the processing of your personal data or the exercise of your right to access public data, you may initiate an investigation with the supervisory authority:

NAIH contact details (https://naih.hu/uegyfelszolgalat,--kapcsolat.html):
address: 1055 Budapest, Falk Miksa utca 9-11.
postal address: 1374 Budapest, Pf:603.
phone number: +36 (1) 391-1400
fax: +36 (1) 391-1400
e-mail: ugyfelszolgalat@naih.hu
web: https://naih.hu/

11.2. Commencement of legal proceedings

If you find that the processing of your personal data is unlawful, you can initiate a civil action against the data controller. The regional court has jurisdiction to decide the case. The lawsuit may, at your discretion, be brought before the competent court of your place of residence (see the list and contact details of the courts at the following link: http://birosag.hu/torvenyszekek).