HST Management Private Limited Liability Company

information on data management related to job advertisements

1. General information about the data management information function

Conia Limited Liability Company, 2200 Monor, Móricz Zsigmond utca 4.utca 4.) (hereinafter the Company or Data Controller), acknowledges the content of this data management information as binding on itself, and undertakes that all data management related to its services is in accordance with this data management complies with the provisions of the information sheet and the applicable legislation. With its data management information, the Company guarantees that it handles personal data in accordance with the relevant legislation and takes all security, organizational and technical measures that protect the security of the data.

2. Purpose of Data Management

- selecting the appropriate future employee from among the applicants for positions advertised by the Company

- in the case of applicants who are not accepted for positions advertised by the Company, but in the event of a possible vacancy later - with the express written consent of the applicant - further registration of the data of registered applicants in order to facilitate the publication of job offers advertised later and the application for them

- in order to fill vacant positions for the purpose of establishing employment at a later date, in the case of non-specific job applicants, the registration of applications received by the Company and the selection of the appropriate future employee from among them.

3. Legal Basis for Data Management

The legal basis for the data management is the written consent of the applicants given by accepting the data management information sheet CXII of 2011 on the right to self-determination of information and freedom of information. according to Section 5 (1) point a) of the Act.

4. Data Controller:

Name: CONIA Kft.
Headquarters: 2200 Monor, Móricz Zsigmond utca 4.
Company registration number: 13-09-202828
Phone : +36-30/503-15-08
E-mail cím: info@coniakft.com

5. The Scope and Management of the Processed Data

In the database created from the provided data, the Data Controller only manages the personal data necessary for recruitment and selection.

The Data Controller asks the applicant not to include data that do not fall within this scope (e.g. hobbies, marital status) or special data (e.g. data related to health, world view, political views) in their CV or motivation letter.

The Data Controller reserves the right to delete content that is incompatible with the purpose of data management.

Mandatory fields for application:

Data groups	Personal data	Purpose of data management
Name	Family name	data required to identify the applicant
	Forename	data required to identify the applicant
Phone number		data required for contact
Residence (Location)		data required for selection
E-mail address		data required for contact
Position you want to fill		data required for selection
Company name		data required for selection
Date		data determining the duration of data management
Signature		data proving consent to data management

Data that can be optionally entered for the application:

Data groups	Personal data	Purpose of data management
CV		data to facilitate selection
Cover letter		data to facilitate selection
Other document		data to facilitate selection
Date of birth		data required to identify the applicant
Income requirement (gross HUF/month)		data to facilitate selection
Relevant experience		data to facilitate selection
Educational attainment		data to facilitate selection
License		data to facilitate selection

The range of data managed in the background database created from the given data:

Data groups	Personal data	Purpose of data management
Name	Family name	data required to identify the applicant
	Forename	data required to identify the applicant
Date of arrival		data required to identify the applicant
Residence	Place	data required for selection
Communication data	Phone number	data required for the purpose of contact
	E-mail address	data required for the purpose of contact
Appendices	CV	data to facilitate selection

	Cover letter	data promoting selection and statistical purposes
	Other documents	data to facilitate selection
Source		data required for statistical purposes
Suitable based on CV		data to facilitate selection
Attending an interview		data to facilitate selection
Test participation		data to facilitate selection
Sent to doctor		data to facilitate selection
Was he medically fit?		data to facilitate selection
Hiring		data to facilitate selection
Rejection based on selection results		data to facilitate selection
He withdrew from the application		data to facilitate selection
Comment		data to facilitate selection
Date of rejection		data to facilitate selection

6. Data Management

The data provided by the applicant are handled exclusively by the recruitment and selection specialists of the Data Controller and the prospective employer.

7. Duration of Data Management

The Data Controller uses the data provided by the applicant from the applicant's consent to filling the position to be applied for, or

- based on the applicant's request - stored in the database for a maximum of 2 years (24 months).

In the case of general, non-specific, applications related to the advertised position, the Data Controller stores the data for 2 years (24 months) from the date of the applicant's consent.

The applicant's personal data will be permanently deleted from the system after 24 months, so it is no longer possible to restore them afterwards.

8. The Data Subject's Rights Related to Data Management

8.1 Right to request information

The applicant can request information from the Data Controller in writing via the contact details provided in point 3.

8.2. Modification and deletion of data

- The applicant can request the modification or deletion of their data recorded in the system at any time. In the event of a deletion request, the personal data will be permanently deleted from the system, and it is not possible to restore them afterwards in any way.

- After deletion or permanent de-identification, the Data Controller stores the following data for statistical purposes: source, date of receipt.

- In addition to these, the Data Controller makes the personal data unidentifiable even if their processing is illegal, if the applicant requests it, if the purpose of the data processing has ceased, if it is incomplete or incorrect, and this state cannot be legally corrected - provided that the deletion is required by other legislation does not exclude it, or the data storage period has expired, or it has been ordered by the court or, for example, the National Data Protection and Information Freedom Authority (hereinafter: the Authority).

8.3. Data lock

The applicant can request in writing that his personal data be blocked by the Data Controller via the contact details provided in point 3. The blocking lasts as long as the reason specified by the applicant makes it necessary. In this case, the Data Controller will continue to store the personal data until the bodies authorized to do so (such as the Authority or the court) are contacted, and then delete them.

8.4. Protest

The applicant may object to data processing in writing via the contact details provided in point 3, if the Data Controller forwards or uses personal data for the purpose of direct business acquisition, public opinion polls or scientific research.

9. Data security

Method of data storage, security of data management:

The Data Controller ensures the saving and archiving of the data, and also observes the procedural rules that are necessary according to the regulations contained in the data protection legislation specified in point 11 of this information.

The Data Controller ensures the protection of the security of data management with technical, organizational and organizational measures that provide a level of protection appropriate to the risks associated with data management, selects and operates the IT tools used in such a way that the managed data:

a) be accessible to those authorized to do so (availability);

b) its authenticity and authentication must be ensured (authenticity of data management);

c) its immutability can be verified (data integrity);

d) it should be accessible only to those entitled to it, and it should be protected against unauthorized access (data confidentiality).

10. Remedies and other information

The applicant can request information about the management of his personal data, as well as request the correction or deletion of his personal data.

At the applicant's request, the Data Controller provides information about the data it manages, the purpose, legal basis, and duration of the data management, as well as who and for what purpose receives or has received the applicant's personal data. The Data Controller shall provide the information in writing in an understandable form as soon as possible, but no later than 25 days after the submission of the request. This information is free of charge if the information requester has not yet submitted an information request for the same area to the Data Controller in the current year. In other cases, the Data Controller may determine reimbursement.

The Data Controller deletes personal data if its processing is illegal, if the applicant requests it, if the purpose of data processing has ceased, if the specified time limit for data storage has expired, or if it has been ordered by the court or the Authority.

The Data Controller will notify the applicant and all those to whom the data was previously forwarded for the purpose of data management of the correction and deletion. The notification will be omitted if this does not harm the applicant's legitimate interests in view of the purpose of the data management.

If the applicant objects to the handling of his personal data, the Data Controller will examine the objection as soon as possible, but no later than 15 days after the submission of the request, and inform the applicant in writing of the result, with the simultaneous suspension of data processing. If the protest is justified, the Data Controller will terminate the data management - including further data collection and transmission - and block the data, as well as notify all those to whom the personal data affected by the protest was previously transmitted, and those who are obliged to take measures to enforce the right to protest.

In case of violation of his rights, or if he does not agree with the decision made by the Data Controller regarding the applicant's protest - within 30 days from the date of its notification - the applicant may also appeal to the court of his place of residence or residence against the Data Controller. The court acts out of sequence in the case.

The applicant can file a complaint with the National Data Protection and Freedom of Information Authority:

Name: National Data Protection and Freedom of Information Authority

Headquarters/ Postal address: 1363 Budapest, Pf.: 9.

Phone: (+36-1) 391-1400 Fax: (+36-1) 391-1410 E-mail: ugyfelszolgalat@naih.hu

The Data Manager excludes responsibility for any damage or disadvantage resulting from any error or malfunction of the data transmission connection.

If, in addition to what is contained in the data protection information, the applicant needs additional information, or has comments or objections regarding the handling of his data, the Data Controller is available at the following contact: info@coniakft.com

11. Relevant legislation:

- CXII of 2011 on the right to information self-determination and freedom of information. law (Infotv.)

- Act V of 2013 on the Civil Code

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free flow of such data, and on the repeal of Regulation 95/46/EC (General Data Protection Regulation or GDPR).