FŐVÁROSI VÍZMŰVEK

DATA CONTROLLING INFORMATION
for applicants

1. Introduction

Fővárosi Vízművek Zártkörűen Működő Részvénytársaság (address: 1138 Budapest, Váci út 182, company registration number) 01-10-042451; **hereinafter referred** to as: **Employer/Data Controller**) devotes particular attention to ensuring that its activities comply with the effective statutory requirements, especially with those laid down in Regulation (EU) 2016/679 of the European Parliament and Council on the protection of natural persons with regard to the management of personal data and the free flow of such data, as well as the repeal of Regulation 95/46/EC (general data protection regulation) (**hereinafter: Regulation**), as well as with the expectations and practices of the water utility service sector.

The Data Controller intends to ensure transparency of its data processing activities by issuing this Privacy Policy Information (hereinafter: **Information**) and by provisions laid down in its related internal policies and regulations, and at the same time inform its potential Employees (**hereinafter: Data Subjects**) of the opportunities provided by their right of self-determination and freedom of information.

Should the Data Subject have general questions regarding data controlling, he/she may directly address the Data Controller's data controlling officer: Károly Gróf: telephone number: 06 1 465 2400; email: **adatvedelem@vizmuvek.hu**; Postal address: Fővárosi Vízművek Zrt. 1397 Budapest, P.O. Box 512.

2. Scope of the Information

The scope of this Information covers the Data Controller's recruitment procedure and typical cases of data controlling related thereto.
The scope of this Information does not extend to data controlling aimed at selecting a given employee for the given job during the recruiting process.

3. Purpose of data controlling:

Purpose of data controlling:

- registration of applicants for concrete positions (database of job seekers), contacting, selection of the right candidate, in case of unsuccessful application registration and information on future vacant positions the candidate is suitable for based on the given data;
- in order to be registered to the database, if no concrete position is available (database of job seekers), registration of later potential candidates providing their details to the Data Controller, contacting in case of a vacant position the candidate is suitable for based on the given data

Scope of the controlled data	Legal basis	Exact purpose of data controlling	Preservation time
Data Subject's name	Consent as legal basis (Article 6, Paragraph	Identification of the Data Subject	Until the Data Subject's consent is revoked / 30 days / 12 months
Email address and telephone number of the Data Subject		Establishing and maintaining contact with the Data Subject	

Curriculum of and other details shared by the Data Subject	(1), Clause a) of the Regulation)	Analysis of suitability for positions, maintenance of the database of job seekers	

4. Data controlling by the Karrier portal

In order to seek out potential employees of the Data Controller, registration of job seekers in the database, personalized service to job seekers, retention of CVs, Karrier has created a portal. The Data Controller reserves the right to use all data provided via the Karrier portal to make decision regarding the employment of the Data Subject or the possibility thereof, to analyze the Data Subject's suitability for the vacant positions and to contact the Data Subject.

There are two ways to submit an application via the Karrier portal:

- full registration by providing the following data:
  Name, email address, telephone number and CV of the Data Subject
- simplified application by providing the following mandatory data:
  Data Subject's name, email address, telephone number, other data shared by the applicant

Scope of the controlled data: Data Subject's name, email address, telephone number, CV, other data shared by the applicant.

Legal basis for data controlling: in all cases the Data Subject's consent ((Article 6, Paragraph (1), Clause a) of the Regulation). Revocation of the consent does not apply to the legality of data controlling before to its revocation.

Duration of data controlling: as a main rule, withdrawal of the consent on behalf of the Data Subject data submitted on the Karrier portal are controlled by the Data Controller for 12 months from the last login, in case of registration requests not confirmed, the duration of data controlling is 30 days.
Data Subjects are entitled to erase their CVs, furthermore, erasing the registration to the Karrier portal is also provided by the Data Controller.

5. Data safety and data transfer

The Data Controller shall make all reasonably expected necessary measures to ensure safety of the data, shall take care of appropriate level of their protection and prevent unauthorized access, alteration, transfer, disclosure, deletion or destruction, as well as accidental destruction or injury.

The Data Controller shall choose and operate IT devices for controlling personal data that guarantee that the controlled data are only accessible by those entitled (availability), the validity of the data is guaranteed (validity of data controlling), integrity of the data can be certified (data integrity), and the data are protected against unauthorized access (data confidentiality).
All IT systems used by the Data Controller to control, process and register personal data can exclusively be accessed by eligible employees, thus the integrity of the data is ensured.

The Data Controller takes care of data safety also by taking appropriate organizational measures.
In case if a data protection takes place - except if it poses no threat to the rights and liberties of natural persons - the Data Controller shall inform the Data Subject and the supervisory authority on the data protection incident without undue delay, but within no more than 72 hours. For the purpose of checking measures related to the data protection incident, informing the supervisory authority and

the Data Subject, the Data Controller shall keep a record containing the scope of personal data related to the incident, the scope and number of the data subjects, time, circumstances and impacts of the incident, as well as the measures taken to avert it.

Data Controllers do not transfer data in connection with the application materials.

6. Rights and legal remedies

Rights	Explanations
Information and access to personal data	Data Subjects are entitled to familiarize and check with their personal data stored by the Data Controller and with the information related to their controlling, and are also entitled to get access to their personal data (e.g. purpose and legal basis of data controlling, when the data are deleted, requesting copies of contract, releasing audio material).
Right to correct or supplement personal data	Data Subjects are entitled to contact the Data Controller in order to immediately correct their inaccurate data (e.g. change of name took place, a new telephone number has been specified).
Right to limit data controlling	Data Subjects are entitled to request the Data Controller to limit controlling of their data, if: • the Data Subject disputes the accuracy of the personal data; in this case the limitation applies to the period available to the data controller to verify the accuracy of the personal data, • the data controlling is illegitimate, and the Data Subject objects the deletion of the data, and requests their limited use instead, • the Data Controller no longer needs the personal data for data controlling purposes, but the Data Subject requests them to submit, enforce or protect legal needs, • the Data Subject objected the data controlling based in insurer's legitimate interest: in this case, the limitation applies to the period, until the determination of whether legitimate reasons of the Data Controller to have priority over the data subject's legitimate reasons.
Right of deletion (right to be forgotten)	The Data Subject is entitled to request the Data Controller to delete his/her personal data without undue delay, if any of these specific reasons are in place: • the personal data are no longer needed for the purpose they were collected or otherwise managed by the Data Controller, • the Data Subject withdraws his or her consent on which the data processing is based and there is no other legal basis for the data processing, • the Data Subjects objects data controlling for reasons related to his/her own situation, and there is no legitimate reason for data controlling, • the Data Subjects objects controlling his/her personal data for the purpose of direct business acquisition, including profiling, if it is related to direct business acquisition,

	• personal data are controlled by the Data Controller illegitimately; • personal data were collected in connection with information society related services offered directly to children. Data Subjects are not entitled to exercise their right of deletion (right to be forgotten), if data controlling is necessary • for the purpose of exercising the right to freedom of expression and information; • to enforce public interest affecting public health care; • for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, if the right to deletion would likely make this data management impossible or seriously jeopardize it; or • *to submit, enforce or protect legal interests.*

The Data Controller and shall inform the Data Subject regarding the actions taken upon his/her request without unnecessary delay, but not later than **within 30 days** as of the receipt of the request. If the Data Subject submitted his/her application electronically, the response shall also be given electronically, unless it was requested otherwise by the Data Subject.

In connection with the legitimacy of controlling their personal data by the Data Controller, Data Subjects may initiate the proceeding of the **Hungarian National Authority for Data Protection and Freedom of Information** (shortly NAIH; address: 1055 Budapest, Falk Miksa utca 9-11.: 1363 Budapest, P.O. Box 9, website: www.naih.hu, telephone: +36 (1) 391-1400, fax: +36 (1) 391-1410, central email address: ugyfelszolgalat+36 (1) 391-1410@naih.hu), or may apply to the court of their place of residence **("right to legal remedy")**.

7. Miscellaneous

The Data Controller reserves the right to unilaterally modify this Data Controlling Policy upon advance notification.

This Data Controlling Policy is valid from September 1, 2023.

Fővárosi Vízművek Zrt.