

DATA PROTECTION NOTICE

(Appendix 3 to the Data Processing Policy)

Effective from: 30/04/2024

Content

1.	Details of the data controller	3
2.	Purpose of the notice	3
3.	General purpose of data processing	3
4.	Processed data.....	4
5.	Data processing procedure	4
6.	Building database for recruitment.....	5
7.	Data processing procedure	5
8.	Data security.....	5
9.	Data transfer, transmission.....	6
10.	Further information	6
11.	Rights of data subjects.....	6

1. Details of the data controller

Designation of the data controller: Digital Service Group Kft.

Registered office: 1126 Budapest, Dolgos utca 2. IV. ép. 2. em. 11. ajtó

E-mail: hunor.tollas@digitalservicegroup.com

Website: <http://digitalservicegroup.com>

Company registration number: 01 09 403370

The staff member overseeing data protection activities (Data Protection Officer): Hunor Tollas

2. Purpose of the notice

The purpose of this data protection notice is to provide information to data subjects in a clear and comprehensible manner regarding the processing of their personal data.

Our company deals with selection, recruitment, personal counselling and related database management of employees. The processing of personal data occurs within the framework of these activities specifically to assist individuals in their job search and to facilitate job placements.

Our task is to assess the employability of candidates for the vacancies and positions specified by employers, in order to meet the expectations of our employer partners who have a contractual relationship with us.

We create a database from the personal data of job applicants, and we process their data in our database - based on the consent of the data subjects - in order to employ them in the future and to contact them with new job offers.

We collect and store personal and sensitive data, transfer personal data to third parties, and conduct any other data processing activities in a manner that ensures unauthorized persons do not have access to such data.

In our data processing activities, we pay special attention to the principles and requirements of the GDPR, specifically the Regulation (EU) 2016/679 of the European Parliament and the Council of 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 (General Data Protection Regulation).

3. General purpose of data processing

The Data Controller deals with recruitment, placement, personal counselling and related database management. Candidates' personal data are processed in the context of these activities for the purpose of facilitating the job search, including the necessary selection procedures, tests and processing of job offers.

In order to employ applicants in the future and to contact them with new job offers, the Data Controller manages the personal data provided in its database.

4. Processed data

4.1 Workforce selection, recruitment

Data subjects: Persons applying directly for a position at Digital Service Group Kft., as well as those contacted by Digital Service Group Kft. staff based on their data uploaded to LinkedIn, Profession.hu, or other publicly accessible databases..

Purpose of data processing: Selecting the workforce who meets the criteria for the job.

Activity	Data category	Legal basis	Purpose	Duration of storage
Recruitment	Data provided in the CV (name, date and place of birth, address, qualifications, schools, previous jobs, telephone number, e-mail address, marital status, children, other data provided, photograph)	Consent	Selecting the workforce who meets the criteria for the job	Until withdrawal of consent/ rejection of the candidate
Recruitment	Name, personal details given at interview	Consent	Selecting the workforce who meets the criteria for the job	Until withdrawal of consent/ rejection of the candidate
Recruitment	name	Consent	Contact	Until withdrawal of consent
	bid amount			

5. Data processing procedure

We are searching candidates for a specific advertised position during recruitment. By applying for the advertisement, the applicant acknowledges the contents of this privacy policy and consents to the processing of their data. Candidates can choose whether to have their details included in our database if they are not selected for the position..

On the basis of the information provided by the applicants and the CVs in our database, we will select the most suitable candidates, with whom we will have an interview in person or by telephone, inform them about the partner offering the position, and then forward their details to the recruiting partner. There is an opportunity to withdraw the consent at the interview. The rest of the selection process is carried out by the partner who advertises the position.

If we find a suitable person for the position based on data from other sources (e.g. LinkedIn, Profession.hu), we will contact them by phone or email, inform them about the data management information and only include them in our database based on their consent.

If you have given your consent to the processing of your personal data in the event that you are not selected for the position, we will process your personal data until you withdraw your consent or for a maximum of 3 years. If the data subject has not consented to the inclusion in the database, his/her data will no longer be kept (we will make the data not linkable to his/her person by transcribing his/her data).

6. Building database for recruitment

Data subjects: Potential employees of Digital Service Group Kft.

Purpose of data processing: Registering competent persons for future recruitment.

Activity	Data category	Legal basis	Purpose	Duration of storage
Building database for recruitment	Data provided in the CV (name, date and place of birth, address, qualifications, schools, previous jobs, telephone number, e-mail address, marital status, children, other data provided, photograph)	Consent	Registering competent persons for future recruitment.	Until withdrawal of consent/ for 3 years

7. Data processing procedure

As described in section 4.1, we retain the personal data of applicants who wish to have their data taken into account in the recruitment process for future vacancies, on the basis of their consent.

The data will be processed until consent is withdrawn or for a maximum of 3 years after consent. The consent can be renewed during the contact.

8. Data security

We ensure the security of the personal data we process through technical and organizational measures, as well as by implementing appropriate procedures.

We protect the data with appropriate measures against unauthorized access, alteration, transmission, disclosure, deletion, or destruction, as well as against accidental loss and damage, and against inaccessibility resulting from changes in the applied technology.

Access to personal data is restricted to employees who require it to carry out their responsibilities.

To keep data secure,

- we assess and take into account potential risks in the design and operation of the IT system, aiming to mitigate them continuously
- we monitor emerging threats and vulnerabilities (e.g. computer viruses, computer intrusions, denial of service attacks, etc.) to take timely action to avoid and prevent them
- we protect IT assets and paper-based information against unauthorised physical access and environmental impacts (e.g. water, fire, electrical surges)
- monitor our IT systems to detect potential problems and incidents
- we take great care to train staff in information security and raise awareness
- reliability is a key criterion in choosing service providers
-

9. Data transfer, transmission

The Data Controller's activities are specifically aimed at transferring or forwarding the personal data of applicants (together with CVs and related documents containing them) to other data controllers (primarily potential employers).

In the case of data transfers abroad, the level of data protection legislation in the third country to which the Controller transfers the personal data may be lower than the level of protection provided by EU legislation. Such transfers to a third country will only be made if the data controller/processor in that country guarantees that enforceable rights and remedies are available to protect the data.

10. Further information

The conclusions that can be drawn about the applicant, in particular that he or she is looking for a job and the type of job he or she wants, counts as personal data. The Data Controller will not pass on this information to other employment agencies.

There are certain details that the applicant must provide in order to use the service. Due to the nature of the services provided by the Data Controller, the voluntary nature of consent is not affected by the fact that the provision of certain data is a condition for the provision of the service.

The Data Controller shall not be liable for any special data (e.g. in a CV) provided without an explicit request. In the event that the applicant discloses any information that, for any reason, qualifies as sensitive data to the Data Controller, the applicant shall provide a separate written consent to the processing of the sensitive data. If the applicant brings such data to the attention of the Data Controller and does not provide an explicit written declaration of consent, the Data Controller shall delete the specific data provided without delay.

11. Rights of data subjects

Each data subject has the right to:

- Be informed about the data processing that affects him before it begins
- Have access to all information related to the data processing that concerns him
- Request the correction of incorrect, inaccurate, or incomplete data.
- Request the deletion (erasure) of their personal data
- Request the restriction of data processing
- Object to the use of data in certain cases, such as for marketing purposes
- Exercise the right to appeal against the data processing

These rights can be exercised by the data subject using the contact details provided in point 1, in writing or by prior arrangement in person. We aim to reply to all requests within the shortest possible time, but no more than 15 business days.

In case of violation of their rights, the data subjects may turn to the National Authority for Data Protection and Freedom of Information.

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

www: <http://www.naih.hu>

e-mail: ugyfelszolgalat@naih.hu