**Privacy Policy**

**on the data processing of personal data of natural persons applying for jobs in connection with the labour recruiting services provided by Grape Solutions Zrt.**

**Preamble**

The purpose of this Policy is to provide information about the personal data processing of Grape Solutions Zrt.as data controller in the frame of its recruitment services for those jobseekers whose personal data are processed during the services.

This Privacy Policy shall not apply to data pertaining to data subjects other than natural persons.

**1. Name of the Data Controller, definition of personal data and Data Subject**

Data Controller is the legal person who alone or jointly with others determines the purposes and means of processing the personal data.

**In relation to this Policy the Data Controller is:**

**Data Controller: Grape Solutions Hungary Zártkörűen Működő Részvénytársaság** (in this Policy hereinafter referred to as: **Data Controller**)

Registered Seat: 1023 Budapest, Árpád fejedelem útja 26-28.

Postal address: 1023 Budapest, Árpád fejedelem útja 26-28.

Registration no.: 01-10-047087

Website: https://grape.solutions

E-mail address: support@grape.hu

Telephone no.: +36-1-880-9200

Data protection officer: dr. Józan Flóra

Availability: Jozan.Flora@nkm.energy

Representative: Gárdonyi Zsuzsa (Gardonyi.Zsuzsa@grape.solutions)

In respect of this Privacy Policy personal data shall mean any information relating to an identified or an identifiable natural person (hereinafter **Data Subject**). An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier (such as name, identification number, location data, an online identifier, or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of that natural person).

**2. Subject of this Privacy Policy and underlying rules of law**

The present Privacy Policy pertains to the **data processing of the Data Controller for recruitment purposes in connection with natural persons taking part in its recruitment services as jobseekers**.

Data Controller during its services conducted on behalf of employers according to the preferences defined by them pursues recruitments in the frame of which Data Controller:

* search potential candidates meeting the criteria of the job opportunity, during which it conducts screening in its own databank and other data bases which it has access to lawfully in harmony with their prevailing contractual conditions;
* conducts a pre-screening (namecheck procedure), registers the Data Subject’s name, birth date or e-mail address in its Namecheck system and forwards these data to the potential employer for the sake to determine whether the employer already knows the Data Subject or not;

- if the pre-screening is successful and the Data Subject may take part in the further recruitment the Data Controller records the Data Subject’s curriculum vitae and professional summary which is prepared by Data Controller with human involvement, in the professional summary only the data provided by the Data Subject in his/her curriculum vitae can be included with unchanged content, no profiling takes place in these summaries (e.g. valuation, analysis, characterization, etc.);

- depending on the subject of the Data Controller’s engagement as part of the recruitments Data Controller conducts interviews and may also perform further pre-screenings during which it may also request from the Data Subjects the fulfilment of tests helping the recruit and fully complying with the legal requirements;

- in respect of the candidates successfully chosen during the recruit process Data Controller may forward certain personal data upon the explicit consent of the Data Subjects towards the potential employer;

- if consented by the Data Subjects the Data Controller records the personal data of the Data Subjects in its own databank for the purpose of forwarding later job possibilities.

Only you shall be liable that the personal data provided by you are true, accurate and up to date. Data Controller explicitly disclose its liability for all consequences arising from data provided incompletely or falsely.

During the recruitment only such statement or disclosure of data can be requested from you which does not infringe your personal rights and material from the aspect of the recruitment. Personal data not related to the recruitment in the lack of data processing purpose cannot be requested. Provision of special category of personal data (such as data on health state, chronic illness, smoking, addiction), their processing shall only take place upon your written consent or under law.

The main legislation pertaining to the above data processing:

* the General Data Protection Regulation 2016/679 of the EUROPEAN PARLIAMENT AND COUNCIL (EU) (April 27, 2016) on the protection of natural persons with regard to the processing personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
* the Act CXII of 2011, on the Right of Informational Self-Determination and on Freedom of Information

**3. Legal grounds of the data processing**

The legal grounds for processing data primarily is the Regulation (EU) 2016/679 of the European Parliament and of the Council (**General Data Protection Regulation**) Article 6 section (1):

* subsection a) (processing under voluntary consent).

Processing of your personal data by Data Controller may take place upon your voluntary and explicit consent which shall be based on your prior notification by the Data Controller. Therefore when you first get into contact with Data Controller or its representative then based on the knowledge of this Policy you shall make a statement whether you consent the processing of your personal data by Data Controller as described in this Policy. **You are entitled – in case of data process based on consent – to withdraw at any time your consent given for the data processing, in which case we will erase your personal data without delay.** The withdraw of the consent makes it impossible for Data Subject to further take part in Data Controller’s recruitment.

**Further details of the data processing, the legal grounds for data processing as per the data processing purposes are defined in the table under section 12.**

**4. Purposes of the data processing**

The main purpose of data processing is the provision of the recruitment services of Data Controller, i.e. searching, screening candidates suitable for its client’s preferences and forwarding the personal file of Data Subject (curriculum vitae) to the Data Controller’s clients for the purpose of establishing employment relationship or other relationship aiming the performance of work.

If separately consented for the purpose of registration in Data Controller’s databank and possible forwarding to the Data Subject of future job opportunities suitable for the professional experience and education of the Data Subject. We do not forward automatically personal data to potential employers, precondition of data forwarding in all events is the prior consent of Data Subject in respect of the subject potential employer.

**Detailed definition of the data processing purposes of the data processing under this Privacy Policy are included in the table under Section 12.**

**5. Scope of data processed, source of the data**

**The detailed definition of the data processed during the data processing under this Privacy Policy are included in the table under Section 12.**

Sources of the data processed: personal data provided/handed over by the Data Subjects.

**6. Persons having access to the personal data, reasons of data forwarding**

**The persons having access to the data defined in this Privacy Policy (persons within the organization of the Data Controller and external recipients) are included in the table under Section 12.**

**In case of the Data Processors detailed under section 9 the reason of the Data Controller’s data forwarding is that the Data Processors can attend their data processing tasks described undersection 9.**

**7. Term of processing, storing personal data**

Data Controller processes the Data Subject’s personal data for the following duration:

* until the withdrawal of Data Subject’s consent, in the lack of withdrawal
* until finishing the recruitment for any reason (e.g. filling in the job or termination of Data Controller’s engagement) which have been conducted for a potential employee in connection with whom the Data Subject has provided his/her personal data to Data Controller.

If Data Subject separately consents to the registration of his/her personal data in the Data Controller’s databank for the purpose that Data Controller may in the future send him/her notification on further job opportunities suitable for Data Subject’s education and qualification offered by other employers or perform pre-screening in connection with potential job possibilities, then Data Controller will process Data Subject’s personal data **until the withdrawal of Data Subject’s consent but maximum until 12 (twelve) months from the date of the consent.** In the lack of such consent or in case of withdrawal of the consent or upon expiry of the 12-month term the personal data provided by the Data Subject will be fully erased from Data Controller’s databank.

**The duration of the data processing under this Policy are included in the table under Section 12.**

**8. Data security**

Data Controller undertakes to ensure the protection of the personal data processed by Data Controller. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Controller shall implement appropriate technical and organisational measures and implement the procedures which ensure that the recorded, stored and processed data are protected, furthermore hinder the destroy, the unauthorized use and change of the data.

Data Controller obliges himself that it will call all third parties to whom Data Controller lawfully forwards or hands over data to comply with the requirements of data security.

Data Controller shall do it best to protect the personal data it processes against unauthorized access, transformation, disclosure, deletion or destruction, accidental destruction or damage. The processed data may only be accessed by the Data Controller, its employees and the data processors deployed by the Data Controller as per access levels, the data shall not be handed over to third persons not having right to access. The employees of the Data Controller and Data Processor shall only have access to the personal data as per scope of job, specific manner and access levels dfined by the Data Controller and the Data Processor.

Data Controller for the sake of security of the IT systems shall protect its IT systems with firewall, and in order to prevent external and internal data loss use virus screens. Data Controller has also arranged for the control of all forms of incoming and outgoing communication for the sake of preventing misuse.

Data Controller and Data Processor qualifies and handles the personal data as confidential data. For the protection of the data files stored electronically in different registers Data Controller ensures that the data stored in the registers – save for the exceptions defined by law – could not be directly connected to the Data Subject.

Data Controller shall ensure a level of data security appropriate to the risk, including among others, in certain cases:

- the pseudonymisation and encryption of personal data,

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services used for the processing of personal data (operation- and development security, protection against intrusion and detection, prevention of unauthorized access),

- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (prevention of data leak, handling vulnerability and incidents),

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (maintaining business continuity, protection against harmful codes, safe storage, forwarding, processing of data, safety training of employees).

When determining the proper level of security expressly such risks arising from the data processing shall be taken into account which result especially from the incidental or unlawful destroy, loss, modification, disclosure or unauthorized access to the personal data forwarded, stored or otherwise processed.

**9. Data processors**

Data processor is such natural person or legal entity which processes personal data on behalf of the Data Controller. In connection with your personal data the following companies, persons proceed as data processors (**Data Processor**):

|  |  |  |
| --- | --- | --- |
| **Data Processor****name, seat, ID data** | **Activity of the Data Processor** | **Personal data processed by the Data Processor** |
| MVM Services Zrt. 1023 Budapest, Árpád fejedelem útja 26-28. | accounting services | data possibly indicated on performance certificates, invoices  |

The data processors are entitled to process the above personal data during the term of their agreement with the Data Controller until the duration related thereof as defined by law.

**10. The rights in connection with data processing and possibility of enforcement of rights and legal remedy**

**10.1. Rights in connection with data processing**

The Data Subject may request from Data Controller the followings:

* to receive information about the facts pertaining to the data processing (before the start of the data processing or during processing),
* access to their personal data (provision of their personal data by Data Controller),
* to have their personal data rectified, or amended,
* save for the cases of compulsory data processing to have the processing of their personal data limited or to have their personal data deleted,
* right to data portability,
* may object against processing their personal data.

The Data Subject may submit its request to the Data Controller as per section 10.2 in writing. Data Controller shall perform the Data Subject’s request within one month by e-mail, letter sent to the availability provided by the Data Subject.

**10.1.1. Right to information (based on Article 13-14 of the General Data Protection Regulation)**

Data Subjects on the availabilities defined under section 10.2 may request information from Data Controller that:

* which personal data,
* under what legal grounds,
* for what purpose,
* from which sources
* for what duration are processed,
* are any data processors deployed, if yes their name, address and activity in relation to the data processing,
* to whom the Data Controller ensured access to or forwarded personal data, when and under what legal regulation,
* the circumstances, impact and the countermeasures taken related to any personal data breach,

**10.1.2. Right to access (based on Article 15 of the General Data Protection Regulation)**

Data Subject is entitled to receive response from Data Controller regarding whether the Data Subject’s personal data are processed by Data Controller and if personal data of the Data Subject are processed get access to their personal data subject to processing together with the following information from Data Controller as per section 10.2 in writing.

Data Controller will provide copy of the personal data undergoing processing to the Data Subject if that is not prohibited by law. If Data Subject has submitted its request by electronic means, then the information shall be provided to the Data Subject in a commonly used electronic form unless otherwise requested by the Data Subject.

**10.1.3. Right to rectification, supplementation (based on Article 16 of the General Data Protection Regulation)**

Through the availabilities defined undersection 10.2 the Data Subject may request in writing from Data Controller to modify any of his/her personal data (for example may change his/her e-mail address or post address or request rectification any of his/her inaccurate personal data).

Considering the purpose of the data processing the Data Subject is entitled to request from the Data Controller the supplementation of any of his/her incomplete personal data undergoing processing.

**10.1.4. Right to erasure (based on Article 17 of the General Data Protection Regulation)**

Through the availabilities defined undersection 5.2 the Data Subject may request in writing from Data Controller the erasure of his/her personal data.

Primarily the erasure of personal data may be requested if our data processing is based on your consent, e.g. you consented that your personal data (telephone number, e-mail) may be processed for contacting purposes. In such an event we erase the personal data.

If you have provided us your personal data for the purpose to perform a contract or under law then the related processing of these personal data will not automatically cease with the termination of the contract and we cannot perform your request for erasure.

In such event we have to process your personal data defined by law further on even after the termination of contract until the duration defined in this Privacy Policy.

**10.1.5. Right to restriction of processing (based on Article 18 of the General Data Protection Regulation)**

Through the availabilities defined undersection 10.2 the Data Subject may request in writing from Data Controller the restriction of processing of his/her personal data (by clearly indicating the restricted nature of data processing and ensuring processing separated from other data).

The restriction shall last until the reason determined by Data Subject makes the storage of the data necessary.

Restriction of data may be requested by the Data Subject for example if he/she thinks that his/her data has been processed by the Data Controller unlawfully, but it is necessary that the data should not be erased for the purpose of any court or administrative procedures initiated by the Data Subject. In such cases until the notification of the authority or the court the Data Controller maintains the storage of the personal data which it only erases thereafter.

**10.1.6. Right to data portability (based on Article 20 of the General Data Protection Regulation)**

Through the availabilities defined undersection 5.2 the Data Subject may request in writing from Data Controller to receive the personal data concerning him/her, which he or she has provided to the Data Controller in a structured and commonly used and machine-readable format and forward these data to another data controller without hindrance from the Data Controller, if

* the data processing is based on consent pursuant to point a) of Article 6 (1) or point a) of Article 9 (2) of the General Data Protection Regulation, or
* based on agreement as per Article 6 Section (1) point b); and
* the data processing is carried out by automatic means.

**10.1.7. Right to objection (based on Article 21 of the General Data Protection Regulation)**

Through the availabilities defined undersection 10.2 the Data Subject may object in writing the processing of his/her personal data pursuant to point f) Article 6 (1) of the General Data Protection Regulation required for the enforcement of rightful interest of the Data Controller or a third party, including profiling based on those provisions. In such event Data Controller shall not further process the personal data, except if the Data Controller demonstrates compelling legitimate grounds for processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

If personal data is processed for the purpose of direct marketing then the Data Subject is entitled to object at any time for the processing of the personal data for this purpose, including profiling if that is related to direct marketing. If the Data Subject objects the processing of the personal data for direct marketing purposes then the personal data may not be processed further on for this purpose.

**10.2. Enforcement of rights, legal remedies in connection with data processing**

**Contacting the Data Controller**

We suggest that before initiating a supervisory- or court procedure first be so kind and contact and send to Data Controller your requests, complaints in connection with the processing of your personal data, thus we can examine and remedy those, and if valid we can perform your requests described under the above section 10.1.

Upon the enforcement of any rights of the Data Subject under section 10.1, upon any request for information, objection to data processing and complaint the Data Controller shall without delay and within the time required by the current rules of law examine the case, make the necessary arrangements in connection with the request and provide information in the matter for the Data Subject. Where necessary taking into account the complexity of the request and the number of the requests this deadline may be extended as defined by law.

Where the Data Subject makes his/her request electronically then information shall be provided as far as possible by electronic form means, unless the Data Subject requests otherwise. If the Data Controller does not take action on the request of Data Subject, Data Controller shall inform the Data Subject without delay and maximum within the deadline defined by law of the reasons for not taking action and on the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

**For the sake of enforcing your rights or if you have any questions, doubt about your data processed by the Data Controller or if you request information or wish to submit a complaint about your data or wish to exercise any of your rights under section 10.1 you may do so as a request by a data subject in letter, e-mail sent to the availabilities of the Data Controller.**

**Initiating a court procedure**

The Data Subject may seek judicial remedy against the Data Controller or against the Data Processor – in relation to the data processing operations falling in the scope of activity of the data processor – if in his/her view the data controller and the data processor engaged or instructed by data controller processed his/her personal data in breach of the provisions of the rules of law applying to processing of personal data or the General Data Protection Regulation.

The law suit shall fall into the competence of the tribunal. The law suit – upon the choice of the Data Subject – may be initiated before the tribunal competent based on the home address or the residential address of the Data Subject.

**Initiating administrative procedure of the supervisory authority**

The Data Subject for the enforcement of his/her rights may initiate an investigation or a supervisory procedure at the National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa u. 9-11., post address: 1363 Budapest, webpage: <http://naih.hu>; tel.: +36-1-391-1400; fax: +36-1-391-1410; e mail: ugyfelszolgalat@naih.hu) on grounds of infringement or the imminent risk of infringement of rights in connection with processing of his/her personal data, especially:

* if in his/her view the Data Controller restricts his/her rights in connection with processing defined under section 10.1 or rejects his/her request to enforce any of such rights (launching an examination), or
* in his/her view during the process of his/her personal data the Data Controller or the data processor engaged by or instructed by Data Controller breaches the provisions on processing personal data defined by law or the mandatory legal regulation of the European Union (requesting procedure by supervisory authority)

**11. Encumbrances**

During the processing of the personal data describe in this Privacy Policy automated individual decision-making, profiling does not take place.

Forwarding of personal data to third countries or international organisations does not take place.

This Privacy Policy can be found at <https://grape.solutions> website.

Data Controller reserves the right to unilaterally amend this Privacy policy for the future. Data Controller will notify the Data Subjects of the amendments on its website and through the Intranet.

**12. Detailed description of the data processing**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Purpose of the data processing** | **Processed personal data, their categories** | **Legal grounds of the data processing** | **Duration of the data processing** | **Persons having access to the data (pls see section 6 also!)****External recipients /if any/** | **Purpose of disclosure (if there is a recipient)** |
| **I. Recruitment services**Provision of recruitment services, i.e. searching and screening of potential candidates meeting the requirements of Data Controller’s clients forwarding of personal material (CVs) of Data Subjects to the Data Controller’s clients for the purpose of establishment employment relationship or other relationship aiming the performance of work | All such personal data which Data Controller must process for its recruitment services, including finding and selecting candidates also. The scope of these personal data are especially: During the pre-screening (namecheck) process: * full name and birth date or e-mail address,

After successful pre-screening: * personal identification data: name, birth date, mother’s name
* education, qualification,
* professional experience (e.g. former work places)
* salary request,
* photo
* e-mail address, telephone number

Furthermore all such personal data which Data Subject voluntarily included in the documents (application, curriculum vitae, motivation letter, education certificates, etc.) sent by the Data Subject to Data Controller or its representative.If the Data Subject separately consents the Data Controller records in the professional summary of the Data Subject the information, data having relevance in respect of the position indicated in the job opportunity which have been disclosed during the personal meetings and discussions between the Data Controller and the Data Subject, plus the result of the tests performed (if any). | the **General Data Protection Regulation** Article 6 section (1) subsection a) - the voluntary consent of the Data Subject | Data Controller processes the Data Subject’s personal data for the following duration: * until the withdrawal of Data Subject’s consent, in the lack of withdrawal
* until finishing the recruitment for any reason (e.g. filling in the job or termination of Data Controller’s engagement) which have been conducted for a potential employee in connection with whom the Data Subject has provided his/her personal data to Data Controller.
 | During the personal data processing conducted by Data Controller in accordance with this Policy such employees of the Data Controller’s HR who take part in the recruitment will have full access to the personal data of the Data Subjects.Furthermore during the recruitment in the selection process other employees of Data Controller may also contribute (e.g. employees conducting the recruit) who will only have access to the Data Subject’s curriculum vitae and professional summary.External recipient:Should the Data Subject be selected during the pre-screening conducted by the Data Controller, then Data Controller will forward the Data Subject’s personal data – curriculum vitae, professional summary, e-mail address, name, birth date, position, telephone number, salary request – to the employer ordering the recruitment for the purpose of performing further selection process. Data Controller will not forward personal data automatically to the potential employers, but the precondition of such data forwarding in all events is the prior consent of the Data Subject in respect of the subject potential employer. After the data forwarding the potential employers will process the forwarded personal data of the Data Subjects during the selection process as independent data controllers according to their own data processing practice, of which the Data Subjects will be informed by the subject employer.  | Potential employers as external recipients – conducting the selection process for the purpose to establish employment relationship |
| **II. Registration in Databank**Upon separate consent registration in the Data Controller’s databank of job seekers and later on forwarding job opportunities to the Data Subject, which harmonize with the qualification and professional experience of the Data Subject  | All such personal data which Data Controller must process for its recruitment services, including finding and selecting candidates also. The scope of these personal data are especially: During the pre-screening (namecheck) process: * full name and birth date or e-mail address,

After successful pre-screening: * personal identification data: name, birth date, mother’s name
* education, qualification,
* professional experience (e.g. former work places)
* salary request,
* photo
* e-mail address, telephone number

Furthermore all such personal data which Data Subject voluntarily included in the documents (application, curriculum vitae, motivation letter, education certificates, etc.) sent by the Data Subject to Data Controller or its representative.Professional summary of the Data Subject in which if the Data Subject separately consents the Data Controller records the information, data having relevance in respect of the position indicated in the job opportunity which have been disclosed during the personal meetings and discussions between the Data Controller and the Data Subject, plus the result of the tests performed (if any). | the **General Data Protection Regulation** Article 6 section (1) subsection a) - the voluntary consent of the Data Subject | Until the withdrawal of Data Subject’s consent but maximum until 12 (twelve) months from the date of the consent | such employees of the Data Controller’s HR who take part in the recruitment will have full access to the personal data of the Data SubjectsData Controller will not forward personal data automatically to the potential employers, but the precondition of such data forwarding in all events is the prior consent of the Data Subject in respect of the subject potential employer.  | - |
| **III. Compulsory data processing based on accountancy and tax legislation** | Scope of processed personal data: name, position and other data to be compulsorily indicated on the performance certificates and the accounting documents | performance of legal obligation as per GDPR Article 6. subsection (1) point c)provisions of Section 166. § subsection (3) and Section 169. § subsection (2) of the Act C of 2000 on accounting, plus Section 78. § of the Act CL of 2017 on taxation | based on the Act on Accounting for 8 years from the date when the data were generatedbased on the Act on Taxation for 5 years from the last day of the calendar year when the calculated tax is due | the authorized employees of the Data Controlleras data processor MVM Services Zrt.As external recipients the persons indicated as purchasers, paying party on the performance certificates, invoices | data processor - accounting servicesexternal recipients – verifying performance and payment of invoices |