

PRIVACY POLICY
IN CONNECTION WITH THE GENERAL PRIVACY POLICY FOR EMPLOYEES OF MVM
COMPANY GROUP BEING IN EFFECT AT GRAPE SOLUTIONS ZRT.
ON DATA PROCESSING REALIZED DURING THE SUPERVISION OF IT TOOLS AND VEHICLES

THE PERSONAL DATA PROCESSED UNDER THIS REGULATION

purpose of processing:	Supervision of the employee behaviour in relation to his/her employment relationship in compliance with Sections 9 and 11/A. § of the Labour Code (Act I of 2012) by Grape Solutions Zrt., as employer (hereinafter: „Employer” or „Data Controller”).
legal grounds of data processing:	The legal grounds of data processing are subsections (1) and (2) of Section 11/A. § of the Labour Code, plus the legitimate interest of Employer.
term of processing:	<p>A) E-mail account: The e-mail account shall be erased at the time of termination of the employment in such way that the IT system prepares a back up copy of the mailbox, which shall be archived including its content for 1 year, or upon initiation of a criminal law procedure until the end of the statutory limitation period, and only the operator and the superior of the employee will have access to it. After the expiry of the archiving period the e-mails will be erased.</p> <p>B) Laptop/Desktop computer, electronic data carrier: Upon termination of employment initiated by employee When employee returns the laptop/desktop computer and electronic data carrier the Employee shall be notified to erase all private nature documents possibly recorded, should employee fail to erase those against such notice the Employer shall not be liable for the processing of these documents. Upon termination of employment initiated by the Employer or extraordinary termination the content of the laptop/desktop computer and electronic data carrier shall not be erased, instead the Employer shall reserve the data carrier after de-assembling or prepares copy of it. The copy shall be archived for 1 year or upon initiation of a criminal law procedure until the end of the statutory limitation period. After the expiry of the archiving period the e-mails will be erased.</p> <p>C) Internet: The IT systems prepare logbooks on the use if the internet. The logbooks shall be archived for 1 year or upon initiation of a criminal law procedure until the end of the statutory limitation period. After the expiry of the archiving period the logbooks will be erased.</p> <p>D) Telephone: In case of calls and SMS made from the telephones provided by the Employer during the supervision the Employer will check the time and term of the calls and the number called on the telephone or based on the detailed list of calls provided by the service provider. The information stored in connection with the use of the telephone shall be archived for 3 years or upon initiation of a criminal law procedure until the end of the statutory limitation period.</p> <p>E) Vehicles: The monthly electronic km-register report of the GPS the Employer shall archive for 3 years or upon initiation of a criminal law procedure until the end of the statutory limitation period, i.e. the limitation period defined by labour law.</p>
list if data and categories:	<p>A) E-mail account:</p> <ul style="list-style-type: none"> ○ content of the non-private nature e-mail; ○ availability of the sending and addressed party; ○ content of the private nature e-mails stored in violation of the rules and related personal data. <p>B) Laptop/Desktop computer, electronic data carrier:</p> <ul style="list-style-type: none"> ○ data, information, content qualifying as personal data stores on the laptop/desktop computer, electronic data carrier. <p>C) Internet:</p> <ul style="list-style-type: none"> ○ address of visited websites, even if they were visited by the

	employee for purposes not related to employment; o names, passwords, other information, content recorded during browsing. D) Telephone: o name, telephone number, time of the call (both official and private calls); o upon possible recording of the call the content of the call (both official and private calls); o name, telephone number and time of the SMS, content of the message (both official and private messages). E) Vehicles: o distance travelled with the vehicle without details (both official and private use).
sources:	personal data recorded by Employer during the supervisions

The legal grounds of the data processing is legitimate interest, the presentation of the legitimate interest is presented in Chapter X of the MVM Company Group Data processing and Data Protection Handbook being in effect at Data Controller and in the prevailing Balancing Test which shall be available at the data protection officer of the Data Controller.

The recording of the above personal data shall take place in compliance with Section 11/A. § of the Labour Code (Act I of 2012) by the Employer during the supervision of the Employee's activity in relation to his/her employment relationship. Should the relevant employee deny the provision of his/her personal data, the right of supervision of the Employer hindering the supervision thereby, then the Employer may apply the legal consequences defined by the Labour Code against the relevant employee. The Employer may check the performance of the provisions, requirements, obligations defined by the effective rules of law, the employment agreement, the Employer's instructions, and the internal rules issued by the Employer - especially Regulations – for the purpose to prevent and prove possibly occurring labour law or disciplinary infringements, offences or crimes.

AUTOMATED DECISION MAKING OR PROFILING

Does the Data Controller apply these?	Information on the logic applied	What are the effects and consequences with respect to the Data Subject
No	Not relevant	Not relevant

RECIPIENT IF ANY

Name of recipients	Purpose of disclosure
Not relevant	Not relevant

WHO CAN ACCESS YOUR PERSONAL DATA?

Primarily the personal data of the Data Subject may only be accessed by the employees of the Data Controller for the purpose to attend their duties. The Supervision may only be performed by the following persons and thus only these persons can access the personal data recorded possibly in connection with the Supervision:

- Security department's executives,
- Security service employee,
- IT security, COB executive, expert employee.

The leading executive of the Data Controller may give access in justified cases based on written request by issuing unique permits to the data recorded during the supervision. The request shall contain:

- name of requestee,
- name of the persons having access to the data base,
- reason for access,
- term of access,
- date and signature of requestee.

DATA SECURITY MEASURES

Data Controller stores the personal data provided by the data subject at the registered seat or registered premises of the Data Controller. Data Controller use the assistance of the data processors listed under **Recipient** for the processing of the personal data of the data subject.

All other provisions are the same as the provisions included in the Privacy Policy handed over at the time of commencing the employment/appointment, plus the provisions of the KIE-16 MVM Company Group personal data processing and data protection guideline.

TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

Name of third country or international organization	Adequacy resolutions of the EU Commission, in the lack of such resolution appropriate safeguards	Binding corporate rules (if relevant)	Derogations pertaining to specific situations (if relevant)
Not relevant	Not relevant	Not relevant	Not relevant

YOUR RIGHTS

Your rights are the same as defined in the Privacy Policy handed over at the time of commencing the employment/appointment, plus the provisions of the KIE-16 MVM Company Group personal data processing and data protection guideline.

The data subject's right to legal remedy before court, complaint addressed to the supervisory authority

Your rights are the same as defined in the Privacy Policy handed over at the time of commencing the employment/appointment, plus the provisions of the KIE-16 MVM Company Group personal data processing and data protection guideline.

DATA CONTROLLER AND DATA PROTECTION OFFICER

Please see in the Privacy Policy handed over at the time of commencing the employment/appointment, plus the provisions of the KIE-16 MVM Company Group personal data processing and data protection guideline.