Data Management Policy
Introduction

MVS Technologies Gépgyártó és Tervező Ltd. (1047 Budapest, Attila út 48., hereinafter the Company, the Controller), as the Controller, acknowledges the content of these legal regulations as binding on it. It undertakes that all data processing related to its activities complies with the requirements set out in these regulations and the applicable legislation.

MVS Technologies Gépgyártó és Tervező Ltd. is committed to the protection of the personal data of its employees, customers, and partners, and considers it extremely important to respect their right to information self-determination. As a Controller, MVS Technologies Gépgyártó és Tervező Ltd. treats personal data confidentially and takes all security, technical and organizational measures that guarantee the security of the data.

In this document, the Controller describes below its data management principles, activities and rules related to the data managed by it. Its data management and data management principles are in line with existing data protection legislation, in particular:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals regarding the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46
- Act V of 2013 on the Civil Code
- Act CXII of 2011 on Informational Self-determination and Freedom of Information (hereinafter the Information Act, Data Protection Act)
- Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services
- Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Economic Advertising
- Act CLV of 1997 on Consumer Protection
- Act CXVII of 1995 on Personal Income Tax
- Act XCIII of 1993 on Occupational Safety and Health
- Act I of 2012 of the Labour Code
- Act CXIX of 1995 on the Management of Name and Address Data for the Purpose of Research and Direct Business Acquisition

1. Scope of the Regulations, Controllers, as well as definitions

1.1. The personal scope of the Regulations extends

a) to all employees of the Company and to work on an ad hoc basis employee used,

b) the processor, and

c) in addition to the above, to any person who has any contractual relationship with the Company.

The material scope of the Regulations extends

a) all data generated by the Company,

b) data managed or processed in the Company's IT system,

c) data created as a result of data processing,

d) all hardware and software devices used by the Company, and

e) data of public interest related to the activities of the Company, generated in the course of its operation or in the public interest.

1.2. Controller

a) MVS Technologies Gépgyártó és Tervező Ltd. headquarters: 1047 Budapest, Attila út 48.; company registration number: 01-09-294875; tax number: 25893928-2-41. Address of actual data management: 1151 Budapest, Mogyoród útja 12-14. internet contact information (and relevant actual data management websites): https://mvs-systems.com/ phone number 1: +36 1 231 7040 e-mail: info@mvs-systems.com independently represented by: Kornacker Gyula director

b) the Employee, a natural person in a legal relationship with the Controller on the basis of an employment contract or other contract that aim employment, in connection with whose activities MVS Technologies Gépgyártó és Tervező Ltd. assumes full responsibility towards the personnel of the parties and third parties.

With reference to the above subsections, under the term 'Controller' shall also mean the Employee, unless otherwise follows from the text of the Regulations.

The Company is not obliged to appoint a data protection officer under Article 37 of the GDPR.

1.3. Definitions

1.3.1. data subject: any natural person identified or identifiable, directly or indirectly, on the basis of personal data;

1.3.2. personal data: any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.3.3. specific data: data on racial origin, belonging to a national or ethnic minority, political opinion, party affiliation, religious or ideological beliefs, party membership, state of health, pathological passion, sexual life

1.3.4. consent: the voluntary and firm expression of a wish by a data subject, based on appropriate information, giving his or her unambiguous consent to the processing of personal data concerning him or her, in whole or in part;

1.3.5. protest: a statement by the data subject objecting to the processing of his or her personal data and requesting the termination of the processing or the deletion of the processed data;

1.3.6. "controller" means the natural or legal person, or any entity without legal personality, which alone or jointly with others determines the purpose for which the data are processed, makes and implements decisions on data processing (including the means used) or enforces them;

1.3.7. data management: any operation or set of operations on data, irrespective of the procedure used, in particular their collection, recording, recording, systematisation, storage, alteration, use, interrogation, transmission, disclosure, coordination or aggregation, blocking, erasure and destruction; and prevent further use of the data, take photographs, sound or images, and record physical identifiers (eg fingerprints or palm prints, DNA samples, irises);

1.3.8. data transfer: making the data available to a specific third party;

1.3.9. disclosure: making data available to anyone;

1.3.10. data erasure: making data unrecognizable in such a way that it is no longer possible to recover it;

1.3.11. data marking: the identification of the data in order to distinguish it;

1.3.12. data blocking: the identification of data to limit their further processing definitively or for a specified period of time;

1.3.13. data destruction: complete physical destruction of the data carrier;

1.3.14. data processing: the performance of technical tasks related to data management operations, regardless of the method and means used to perform the operations and the place of application, provided that the technical task is performed on the data;

1.3.15. data processor: a natural or legal person or an organization without legal personality who, on the basis of a contract concluded with the Controller, including the conclusion of a contract on the basis of a provision of law, processes the data;

1.3.16. data filing system: any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

1.3.17. third party: a natural or legal person or an organization without legal personality who is not the same as the data subject, the Controller or the processor;

1.3.18. third country: any state that is not an EEA state.

2. Principles of data management

The Company carries out its Data Management activities for the reasons set out in this prospectus. The current director of the Company, in cooperation with the managers of the Company, determines the tasks of the employees related to data management. The purpose of their activities is to ensure the accuracy of the data in all phases of data processing in a lawful and fair manner, and to ensure the protection of the personal data of the data subject in the event of unauthorized access, alteration, transmission, deletion or destruction. Other organizations involved in data

management related to the Company, resp. business representatives are obliged to keep the information disclosed as a business secret.

Personal data can be processed

- with consent, or
- if it is ordered by law or - based on the authorization of law, in the scope thereof - by a decree of a local government for a purpose based on the public interest (mandatory data management).
  Personal data may be processed if the investigation of the information is impossible or proportionate and the processing of personal data is necessary to fulfil the legal obligation to the Controller or requires the approval of the Controller or third party rightsholders and the right to personal data protection proportionate to the restriction.

If the personal data has been collected with the consent of the data subject, the Controller may use the collected data

- for the purpose of fulfilling the legal obligation applicable to him or her, unless otherwise provided by law, or
- for the purpose of enforcing the legitimate interest of the Controller or a third party, if the exercise of such interest is proportionate to the restriction of the right to the protection of personal data

without further specific consent and after the withdrawal of the data subject's consent.

Personal data may only be processed for a specific purpose, to exercise a right and fulfil an obligation. At all stages of data processing, this purpose must be met, and the collection and processing of data must be fair.

Only personal data may be processed that is essential for the purpose of the data processing, suitable for the purpose and for the time and for the time necessary to achieve the purpose.

Personal data may only be processed with informed consent.

The data subject shall be informed before the start of the data processing that the data processing is based on consent or is mandatory. The data subject shall be informed in a clear, comprehensible, and detailed manner of all facts relating to the processing of his data, in particular the purpose and legal basis of the data processing, the person authorized to control and process the data, the duration of the data processing and for the purpose of fulfilling a legal obligation to the Controller or a legitimate interest of a third party, and who may have access to the data. The information should also cover the data subject's rights and remedies.

During data management, it must be ensured that the data is accurate, complete, and up-to-date, and that the data subject can be identified only for the time necessary for the purpose of data management.

Personal data may be transferred to a controller or processor processing data in a third country if the data subject has given his or her explicit consent or the conditions for data processing set out above are met and an adequate level of protection of personal data is ensured in the controlling and processing of transferred data in the third country. The transfer of data to the EEA States shall be deemed to take place within the territory of Hungary.

3. Data security and information security rules

The Controller and the Processor shall take appropriate technical and organizational measures to take into account the state of science and technology and the costs of implementation, as well as the nature, scope, circumstances and purposes of data processing and the varying likelihood and severity of risks to the rights and freedoms of natural persons to guarantee a level of data security appropriate to the degree of risk, including, inter alia, where appropriate:

- pseudonymisation and encryption of personal data;
- ensuring the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data;
- in the event of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner;
- a procedure for regular testing, assessment, and evaluation of the effectiveness of the technical and organizational measures taken to ensure the security of data management;
- the processed data must be stored in such a way that they cannot be accessed by unauthorized persons. In the case of paper-based data carriers, by establishing the order of physical storage and archiving, in the case of data processed in electronic form, by applying a central rights management system;
- the method of storing the data by the IT method must be chosen in such a way that their erasure can be carried out at the end of the erasure period or, if necessary for other reasons, considering the possible different erasure period. Deletion must be irreversible;
- paper-based media must be deprived of personal data by means of a shredder or by an external shredder. In the case of electronic media, the rules on the disposal of electronic media shall provide for physical destruction and, where necessary, for the secure and irrevocable erasure of data in advance.

The Controller takes the following specific data security measures:

- to ensure the security of personal data processed on paper, the Controller applies the following measures (physical protection):

1. Store documents in a safe, lockable, dry room.
2. The building and premises of the Controller are equipped with fire protection and property protection equipment.
3. Personal data may be accessed only by authorized persons and may not be accessed by third parties.
4. In the course of his or her work, the data processing employee of the Controller may leave the room where the data processing takes place only by closing the data carriers entrusted to him or her or closing the given room.
5. Where personal data processed on paper are digitized, the rules governing digitally stored documents shall apply.

- IT protection

1. The computers and mobile devices (other data carriers) used in the data management are the property of the Controller or the Employees.
2. Data on computers can only be accessed with a username and password.
3. The central server machine can only be accessed with appropriate authority and by designated persons.
4. To ensure the security of digitally stored data, the Controller uses data backups and archives.

5. The computer system containing the personal data used by the Controller is equipped with virus protection.

4. The scope of personal data processed and the characteristics of data management.

The data management of the activities of MVS Technologies Gépgyártó és Tervező Ltd. is based on voluntary consent. However, in some cases, the handling, storage, and transmission of a given set of data is made mandatory by law, of which it notifies its employees, customers and partners separately.

4.1. General provisions in connection with each data management activity, use of the services provided by the Controller

Generally, the management of all data related to the data subject in the data management activities and services provided by the Controller is based on voluntary consent [Article 6 (1) (a) GDPR], and the general purpose is to ensure the provision of the service and to keep in touch.

The above general rule is supplemented by data processing based on other legal bases, such as data processing required by law, of which the Controller informs the data subjects during the definition of each data processing.

Generally,

- for some services it is possible to provide additional data that will help to fully understand the needs of the data subject, but these are not conditions for the use of the services provided by the Controller,
- personal data provided during any data management activity is stored by the Controller in separate data files, separately from other provided data. These data files may only be accessed by the Authorized Employee (s) of the Controller,
- the Controller does not transfer individual data or all data files to third parties without the prior consent of the data subject, except for statutory mandatory data transfer, and takes all security measures to prevent unauthorized access to the data,
- the data subject may modify, delete and / or block the data recorded and stored during any data management activity, as well as request detailed information about the data management activity, by sending a request to the following e-mail address, if no other contact information is specified: info@mvs-systems.com
- the provision of the data to be provided during each data management activity by the data subject is a condition for the use of the services provided by the Controller.

4.2 One-time information request

The Controller allows data subjects to request information from the Controller by providing their data detailed below.

The request for information is based on voluntary consent [Article 6 (1) (a) GDPR].

Data subject: Any natural person who contacts the Controller and requests information from the Controller in addition to providing his or her personal data.

Scope and purpose of data processed:

name - identification

email address - contact

content of the question - answer

The purpose of data management is to provide the data subject with appropriate information and to keep in touch.

The activity and process involved in data management are as follows:

- the data subject may consult the Controller about the Controller's products, services and / or other related issues through or in a manner provided to him / her by the Controller.

- the data provided to the Controller via the website will be sent by e-mail.

- the Controller answers the data subject's question and sends it to him / her in the same way as the information request was received unless the data subject provides otherwise.

- the data subject, in accordance with the purpose of the data processing, voluntarily consents to the Controller contacting him / her during the request for information to clarify or answer the question.

Duration of data management: until the goal is achieved. If the request for information and / or the provision of information has legal effect or affects the data subject or the Controller to a similarly significant extent, the Controller shall process the data at the respective limitation period.

4.3 Request for quotation

The Controller allows interested parties to request a quote from the Controller by providing their data detailed below.

The request for quotation is based on voluntary contributions [Article 6 (1) (a) GDPR].

Data subject: Any natural person who requests an offer from the Controller in connection with a given service, providing his / her personal data.

Scope and purpose of data processed:

name - identification

telephone number - contact

email address - contact

question / request content - answer

The purpose of data management is to provide the data subject with an appropriate offer and to keep in touch [Article 6 (1) (a) GDPR].

The activity and process involved in data management are as follows:

The data subject shall send his / her data to the Controller via the means or in the manner provided to him / her by the Controller.

The data provided to the Controller via the website will be sent by e-mail.

The Controller shall prepare a suitable offer at the request of the data subject, or if the information necessary for the submission of the offer is obtained, the Controller shall contact the data subject and prepare the offer in possession of the information and send it to him/her in the same way as the request for quotation, if otherwise it does not provide.

In accordance with the purpose of data processing, the data subject voluntarily consents to the Controller contacting him / her during the request for quotation to clarify the offer or to confirm the data subject's order.

Duration of data management: until the expiry of the offer.

4.4 Data management related to the conclusion of an agreement and the performance of a service

The Controller concludes an agreement in advance for the provision of each of its services.

The conclusion of the agreement is based on voluntary consent.

Data subject: All natural persons, as well as persons acting on behalf of the organization (representative, contact person) who enter into an agreement with the Controller - in addition to providing their personal data - on the use of the Controller's services.

Scope and purpose of data processed:

name - identification

email address - contact

the name of the organization represented - identification, invoicing

telephone number - contact

name of the service ordered - data required for performance and invoicing

rights and obligations - content of the agreement

billing address (name, country, zip code, city, street, house number, additional data) - data required for billing

payment method - information required for invoicing

final amount - data required for financial performance

The purpose of data management is to identify the data subject, to provide the data subject with appropriate services in accordance with the provisions of the agreement, and to maintain contact [Article 6 (1) (a)-(b) GDPR].

The activity and process involved in data management are as follows:

The data subject shall notify the Controller of the acceptance of the Controller's offer through the way or in the manner provided by the Controller and available to the data subject.

The Controller shall work out the details of the agreement together with the data subject, considering the content of the accepted offer (this includes the application of the general contractual condition).

He / she provides the data subject to the Controller for the creation of the agreement and its contractual performance and enters into the agreement with the Controller voluntarily and without influence.

The Controller shall record the agreement in the electronic and / or paper-based registration system set up for this purpose.

The Controller may notify the data subject of each step of the execution process.

In accordance with the purpose of the data management, the data subject voluntarily consents to the Controller contacting him / her via the given contact details to discuss the details of the performance and / or related issues.

Duration of data processing: lasts until the validity of the rights and obligations arising from the legal relationship in connection with which the Controller processes personal data expires in respect of data that are documented and the document supports the accounting, the data processing period is Act C of 2000 Pursuant to Section 169 (2) for at least 8 years [Article 6 (1) (c) GDPR].

4.5 Data managed through continuous, regular contact with the data subject

The Controller shall ensure that the Company is in constant or regular contact with the data subject in various ways and forums. By way of example, electronic communication such as e-mail, postal or telephone contact, etc. (For example, correspondence with a subject.)

The legal basis for data processing is the voluntary consent of the data subject [Article 6 (1) (a) GDPR]. If the Controller and the data subject enter into an agreement with each other, for example on the use of a service of the Controller, the legal basis of the data processing is based on the conclusion of a contract [Article 6 (1) (b) GDPR]. Contact, so the processing of the relevant data may be based on the legitimate interest of the data subject, third party or the Controller, as well as on other legal grounds specified by law, for example, it may also be mandatory by law [Article 6 (1) (c)-(f) GDPR]. Upon request, the Controller shall inform the data subject of the legal basis on which he or she manages his or her data.

Data subject: All natural persons, including natural persons acting on behalf of an organization, who, in addition to a one-off request for information, are in constant or regular contact with the Controller.

Scope and purpose of the data processed:

name - identification

telephone number - contact

email address - contact

question, other data provided by the data subject - answer

The purpose of data processing is to contact the data subject, to answer and resolve any questions, requests, and other issues, and to obtain the information necessary for the contractual performance of the agreement between the parties.

The activity and process involved in data management are as follows:

The data subject shall contact the Controller orally (in person, by telephone) or in writing (by post, e-mail) or keep in touch with the Controller through a means or manner provided by the Controller, and shall address a question, request, or other matter to the Controller towards.

Based on the content of the contact and the laws and internal regulations, the Controller will take the necessary steps and inform the data subject.

Duration of data management:

- until the goal is achieved,
- if required by the interest or fulfilment of an obligation of the data subject or a third party or the Controller, the data processing lasts after the realization of the purpose, until the termination of the interest or the fulfilment of the obligation
- if the duration of the data processing is mandatory by law based on the method of data processing or otherwise, the Controller shall process the data for the period specified in the relevant legislation.

4.6 Data Management on the Website

The data management of the activity of the https://mvs-systems.com/ website is based on voluntary consent [Article 6 (1) (a) GDPR]. In some cases, however, the handling, storage and transmission of a given set of data is required by law, of which we will notify the visitors and users separately.

4.6.1 Data of the visitors of the https://mvs-systems.com/ website

The purpose of data management: when visiting the website, the website hosting provider records the visitor data to check the operation of the service and prevent abuse.

Legal basis for data management: the consent of the data subject [Article 6 (1) (a) GDPR] and the provisions of Act CVIII of 2001 on certain issues related to information society services Pursuant to Section 13/A. § (3) [Article 6 (1) (c) GDPR].

The scope of data managed: date, time, IP address of the user's computer, address of the visited page, address of the previously visited page, data related to the user's operating system and browser.

Google Analytics' web analytics software and external server help you independently measure and audit website traffic and other web analytics data. The Controller can provide detailed information on the management of measurement data at www.google-analytics.com.

To provide customized service, external service providers use a small data package on the user's computer, a cookie is placed and read back. If the browser returns a previously saved cookie, the service providers that handle it have the option to link the user's current visit to the previous ones, but only for their own content.

Duration of data management: 2 years from the date of viewing the website.

The https://mvs-systems.com/ website web beacons are not used.

4.6.2 Keeping in touch with customers

The purpose of data management:

The Company's website provides an opportunity for prospective partners to establish direct contact with the Company's designated employees. To use the customer contact point, you must accept the privacy statement on the website.

Scope and purpose of the data processed:

name /company name - identification

telephone number - contact

email address - contact

Legal basis of data management: Act CXII of 2011 on freedom of information and the right to information self-determination [Article 6 (1) (a)-(c) GDPR]. The data management of the partners is considered customer data, so it is not reported to the register of the data protection authority.

Duration of data management: Until the consent of the registered partner is withdrawn.

4.6.3 Facebook remarketing

The Controller places a set of codes on the website, or on any of its sub-pages, the purpose of which is to make the Controller's advertisement available to the user visiting the given website while using Facebook. The Facebook remarketing code set does not collect, store or transmit personal information. More information on the use and operation of the code set can be found at www.facebook.com.

4.6.4. Google Adwords remarketing

The Controller places a set of codes on the website, or on any of its sub-pages, the purpose of which is to make the Controller's advertisement available to the user visiting that website while browsing the Google Display Network sites and / or the Controller, or They search Google for terms related to their data management services. The code set does not collect, store or transmit personal data.

For more information on how to use and operate it, visit http://support.google.com.

4.6.5. Community sites

The fact of data collection, the scope of data managed: Facebook / Google + / Youtube / Instagram, etc. registered name on social networking sites and the user's public profile picture.

Data subject: All data subjects who have registered on Facebook / Google + / Youtube / Instagram, etc. social networking sites and "liked" the website.

The purpose of data collection: To share or "like" certain social elements, products, promotions or the website itself on social media sites.

Duration of data processing, deadline for deletion of data, possible persons entitled to access the data description of the Controllers and the data subjects' rights related to data processing: Data management is carried out on social networking sites, so the duration and method of data management, as well as the possibilities of deleting and modifying data are governed by the regulations of the given social networking site.

Legal basis for data processing: the voluntary consent of the data subject to the processing of his or her personal data on social networking sites [Article 6 (1) (a) GDPR].

4.7 Data management related to job advertisements (recruitment)

The Controller or the head-hunter will receive the CVs of the applicants at the e-mail addresses and by post provided on their websites. Paper-based and electronically received CVs are treated equally.

In the case of advertised job advertisements, the Controller or the head-hunter informs the candidates about the provisions of these regulations, and in case of applying for an unpublished position, the Controller or the head-hunter sends a reply letter to the applicant informing about the provisions of these regulations.

Applicants for the Controller's job advertisement will receive an electronic message informing them of the Controller's data management and the status of his / her application.

In the message, applicants can request additional information or the deletion of their personal data at the e-mail address.

The Controller or the head-hunter will not collect any further data on the applicants other than the submitted application and then the selection procedure.

Legal basis for data processing: Article 6 (1) (a) GDPR. By sending his / her CV, the data subject consents to the Controller managing his / her CV in accordance with these regulations.

The purpose of data management is to select a suitable prospective employee to fill vacancies for the purpose of establishing an employment relationship later.

Duration of data processing: The Controller and / or the head-hunter first handles the personal data until the end of the selection and then - if no request for deletion is received from the data subject - for another 1 year.

Scope of data managed:

The following data of the applicant: Name, address, place and time of birth, mother's name, contact details, data on education and training, photos, language skills, internships, previous jobs, hobbies, and other data provided by the data subject.

Data subject: All data subjects applying for a job vacancy / application.

Potential recipients: The Controller does not forward the documents received directly from the data subject during the application (CV, motivation letter, application material) to third parties. When the Controller using a third party for recruiting, then the third party (head-hunter) forward the documents directly from the data subject to the Controller.

4.8. Data Processing Activities of the Company

Pursuant to the contractual terms of the agreements on the provision of services concluded by the Controller to fulfil its obligations, the principal may transfer data or process personal data on behalf of the Controller's Client. The agreement concluded with the principal defines the conditions for the processing of and access to the personal data for which the Controller is responsible as a Processor.

The Controller and the person with access to the personal data handle the transmitted personal data only in accordance with the instructions of the principal.

The principal is legally responsible for the activities of the Controller as a Processor. The Controller, as Processor is liable for damages caused by data processing only if it has not complied with the obligations specified in the GDPR, which are specifically imposed on the Processors, or if it has disregarded or acted contrary to the principal's lawful instructions.

The Controller, as a Processor, does not have any meaningful decision-making concerning data management.

The Controller, as a Processor, is obliged to keep a record of the data management activities performed on behalf of the principal, which it can present to the data protection authority at any time, if necessary.

As a Processor, the Controller undertakes to keep confidential the personal data that come to its knowledge during the performance of its data processing activities and any other information that comes to its knowledge during the data management or data processing activities of the principal and to use them only for the specified tasks.

The Controller, as a Processor, is obliged to duly inform the Employees involved in the performance of data processing activities.

The legal basis for the processed data and the details of the lawful processing, in particular the consent of the data subjects to the transfer of their data to a third party, are set out in the client's current data protection policy.

Otherwise, the principles and regulations of these regulations apply.

Legal basis for data processing: Article 6 (1) (f) GDPR.

Purpose of data processing: performance of the contract by the principal

Duration of data processing: until the termination of the contract

Data subject: data managed by the principal that are transmitted to the Controller pursuant to the performance of the contract between the principal and the Controller

5. The data security rights, and legal remedies of the person involved in data management

5.1. Rights of holders of personal data

Natural persons whose personal data are processed by the Controller for any reason have the following rights regarding the data processing of the Controller:

a.) the right to information;

b.) the right to rectification;

c.) the right to be forgotten;

d.) the right to restrict data processing;

e.) the right to data portability;

f.) the right to protest.

The owner of the personal data may exercise the right specified in this chapter by submitting a request to the Controller. The owner of the personal data may submit the application electronically, on a paper basis using the universal postal service, or on paper by handing it over to the Controller's actual data management address to a senior official or employee authorized to represent the Controller.

The person entitled to receive the request is obliged to forward the request to the Controller's Data Management Officer for administrative purposes immediately upon receipt. The Controller shall examine the request - immediately upon receipt thereof - and if it finds that it was received from a manifestly unfounded or unauthorized person, it shall reject its substantive examination. If the request is not submitted by a manifestly unfounded or authorized person, the data protection officer shall examine the merits of the request. The Controller shall, no later than 30 days after

receipt of the request, notify the applicant of the assessment of the request (rejection of the request or execution of the request) and of the measures taken or initiated.

5.1.1. Right to rectification

If the Controller inaccurately or incompletely handles any personal data of the data owner, the Controller may request the Controller to correct the inaccurately processed personal data immediately or to supplement the incompletely processed personal data based on the data provided and verified by the data subject.

The owner of the personal data (or his / her authorized and certified proxy) may submit his / her request for rectification by sending it to the Controller. If the personal data is contained in a public document (e.g., an official card), the applicant is obliged to present or provide a copy of the public document certifying the content of the personal data to the Controller.

5.1.2. The right to be forgotten

The owner of the personal data is entitled to request the Controller to delete his / her personal data from all records of the Controller. Upon receipt of this request, the Controller shall delete the personal data requested immediately if one of the following reasons exists:

- personal data are not required for the purpose for which the data were processed;

- the data subject has withdrawn his / her consent to the processing and there is no other legal basis for the processing;

- it is proved that the personal data was processed unlawfully by the Controller;

- due to a legal obligation, the Controller is obliged to delete personal data.

The owner of the personal data may submit his / her request for deletion by sending it to the Controller.

The Controller may refuse to delete personal data if one of the circumstances specified in Article 17 (3) of the GDPR exists.

5.1.3. Right to restrict data management

The owner of personal data is entitled to request the Controller to restrict the processing of data concerning his personal data if:

- the owner of the personal data disputes the accuracy of the personal data collected and stored by the Controller for the period of time to verify the accuracy of this data;

- The processing of data by the Controller is illegal and the owner of the personal data objects to the deletion of the personal data collected and stored;

- the purpose of the data processing has ceased, and the Controller does not need the personal data collected and stored, but the owner of the personal data requests further (limited) data processing in order to submit, validate or protect his / her legal claim;

- the holder of the personal data exercises his right to restrict data management for the duration of the examination of the lawfulness of the right of objection.

The owner of the personal data (or his / her authorized and certified proxy) may submit his / her request for the restriction by sending it to the Controller.

The Controller is only entitled to store personal data that is not subject to the restriction. The Controller is entitled to process personal data subject to the restriction only to obtain the prior written consent or to present, enforce or protect the legal interest of the data subject and in the important public interest of the European Union or its Member State.

If the conditions for the restriction of personal data do not exist, the Controller shall lift the restriction and shall inform the owner of the personal data in advance.

5.1.4. Right to data portability

Regarding personal data processed by the Controller in an automated manner with the consent of the data owner, the data controller may request the Controller to make the personal data provided by him / her available to the Controller in electronic format, as defined in Article 20 (1) GDPR.

When transferring the collected and stored personal data in electronic form, the Controller is obliged to consider that the owner of the personal data is entitled to transfer the collected and stored personal data electronically to another Controller or to ask the Controller to send this personal data directly to the other Controller.

The owner of the personal data (or his / her authorized and certified proxy) may submit his / her request for data transfer by sending it to the Controller.

5.1.5. Right to protest

The owner of the personal data may object to the data processing of his / her personal data by the Controller if the Controller performs the data processing to enforce the legitimate interest of the Controller or a third party.

The owner of the personal data (or his / her authorized and certified proxy) may submit the request for protest by sending it to the Controller.

Following the acceptance of the statement of objection by the Controller, the Controller is not entitled to process the personal data concerned to enforce the legitimate interests of the Controller or a third party, unless the Controller proves that the processing is justified by overriding legitimate interests. rights and freedoms or relating to the submission, exercise, or defence of legal claims.

5.2. Dealing with privacy incidents

The Company acknowledges that a data protection incident may cause physical or non-material damage to natural persons in the absence of appropriate and timely action. To deal with data protection incidents, it shall keep a data protection incident log in which the circumstances of the data protection incident shall be recorded by the Data Protection Officer within a maximum of 72 hours of the incident being reported.

5.3. Remedies

The person concerned may receive information on the handling of his or her data in person, after prior registration, from Monday to Friday, from 9 am to 4 pm, without voice recording, and may request that his or her personal data be corrected and deleted or blocked. The Controller shall investigate the complaint as soon as possible, but not later than within 15 days from the submission of the request and shall provide written information. If inaccurate personal data is registered by the Controller, the Controller shall amend it if true personal data is available.

The Controller deletes the personal data if:

- if its handling is illegal
- is incomplete or incorrect and this condition cannot be legally remedied
- the data subject requests
- the purpose of data processing has ceased, or the period of data storage specified by law has expired
- this has been ordered by a court or authority

Personal data subject to the obligation to delete shall be blocked by the Controller instead of deletion if the data subject so requests or based on the available information it can be assumed that the deletion would harm the data subject's legitimate interests. Personal data blocked in this way can only be processed if there is a data management purpose that precludes the deletion of personal data.

The Controller may transfer the legally necessary data that are necessary for the purpose of data management:

- to settle legal disputes for bodies entitled under the law
- for the protection of national security, national defence, and public safety, for the prosecution of public prosecutions, to the competent authority
- under other legal provisions

If the data subject does not agree with the decision or information of the Controller regarding the processing of his / her personal data, or if the Controller fails to meet the deadline for reply specified by law, the data subject may apply to a court or the National Data Protection and Freedom of Information Authority within 30 days of the notification of the decision or the failure to meet the deadline. The trial falls within the jurisdiction of the tribunal. If the court grants the request, the Controller shall be instructed to provide the information, to correct, block, delete the data, to annul the decision made by the automatic data processing, to consider the right of the data subject to protest, or may require the release of data.

In case of violation of the rights of the data subject or remarks, you can make a statement or contact you can contact the following authorities:

National Data Protection and Freedom of Information Authority: 1055 Budapest, Falk Miksa utca 9-11.

MVS Technologies Gépgyártó és Tervező Ltd. (1047 Budapest, Attila út 48.)

Budapest, 16/07/2024