

## Information leaflet about processing of personal data

In accordance with articles 13 and 14 of the regulation (EU) 2016/679 OF the European Parliament and of the Council of 27 April 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 (hereafter: GDPR) the Controller hereby provides the following information for the data subjects about the processing of personal data:

	<b>Controller</b>	<b>Data Protection Officer</b>
Name:	<b>MVM XPert Zrt.</b>	<b>Kovács István</b>
Postal address:	1601 Budapest, Pf. 83.	1031 Budapest, Szentendrei út 207-209.
E-mail:	kommunikacio@mvmxpert.hu	dpo@mvm.hu
Telephone:	+36 1 414 3200	+36 1 304 2000
Fax:	+36 1 415 5815	
Web:	<a href="http://www.mvmxpert.hu">www.mvmxpert.hu</a>	
Registered office:	1158 Budapest, Rákospalotai körvasút sor 105-106.	

### Legislation serving as basis for processing

Regulation (EU) 2016/679 OF the European Parliament and of the Council of 27 April 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) (hereafter: "GDPR", the text of the legislation in force is available on the link below :

[http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC))

Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereafter: "Privacy Act"; the text of the legislation in force is available on the link below:

[http://njt.hu/cgi\\_bin/njt\\_doc.cgi?docid=139257.338504](http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.338504))

Under GDPR '**personal data**'

means any information relating to an identified or identifiable natural person ('data subject'); 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;

**'recipient'**

means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

**PERSONAL DATA**

<b>purposes of the processing:</b>	in the Appendix
<b>legal basis for the processing:</b>	in the Appendix
<b>period for which the personal data will be stored:</b>	in the Appendix
<b>list and categories of personal data:</b>	in the Appendix
<b>source of personal data:</b>	in the Appendix

If the legal basis for processing specified in the **Appendix** is legitimate interest, the legitimate interest is described in the **Appendix**.

In principle the provision of the personal data listed in the Appendix depends on the free choice of the data subject. If the provision of the personal data listed in the Appendix is a statutory or contractual requirement, or a requirement necessary to enter into a contract the data subject is obliged to provide the personal data listed in the Appendix, the consequences of failure to provide such data may be:

- data request for the purpose of discharging legal obligations: discharging the legal obligation may become impossible
- data request for the purpose of entering into a contract: failure to conclude a contract
- data request for the purpose of using services: refusal to provide services
- data request for security purposes: limit or exclude access

**Automated decision-making or profiling**

<b>Is it applied by the Controller?</b>	<b>Meaningful information about the logic involved</b>	<b>Significance and the envisaged consequences of such processing for the data subject</b>
No	Not relevant	Not relevant

**Recipient if applicable**

<b>Names of recipients</b>	<b>The purposes for which, the personal data is disclosed</b>
In the Appendix	In the Appendix

## WHO CAN ACCESS YOUR PERSONAL DATA?

In principal the employees the Controller can access the personal data of the data subjects for the purpose of discharging their duties. So personal data can be accessed for example by the Controller's staff in charge of operating the filing system for administration purposes, or by its human resources staff for preparing labour contracts.

The Controller may only disclose personal information to state agencies in exceptional cases. So, for example if a court proceeding is initiated in a legal dispute between the Controller and the data subject and it is required to hand over to the court documents containing the data subject's personal data, the Controller is requested by the police authority to disclose personal data of the data subject for the purposes of an investigation. Furthermore for example personal data may also be disclosed to Controller's legal counsel providing legal representation in case there is a legal dispute between the Controller and the data subject.

## DATA SECURITY MEASURES

The Controller stores the personal data provided by the data subject at its registered seat or branch. Controller uses the services of the data processor indicated in the Appendix for processing the personal data of the data subject.

The Controller takes the necessary information security measures to protect the data subject's data among others from unauthorized access or from unauthorized alteration. So, for example accesses to data stored on the servers are logged, which ensures that it can be checked who and when accessed a specific personal data. The Controller takes adequate organizational measures to prevent disclosing personal data to an undetermined number of people.

## DISCLOSEURE BY TRANSMISSION TO A THIRD COUNTRY OR AN INTERNATIONAL ORGANIZATION

The name of the third country or the international organization	The Commission's adequacy decision or guarantees	Binding corporate rule (if applicable)	Derogations for specific situations (if applicable)
Not relevant	Not relevant	Not relevant	Not relevant

## YOUR RIGHTS

### Under article 15 of GDPR data subjects may request access to their personal data as follows:

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) the right to lodge a complaint with a supervisory authority;
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

### Under article 16 of GDPR data subjects may request rectification of their personal data from the Controller as follows:

*The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.*

### Under article 17 of GDPR data subjects may request the erasure of their personal data from the Controller as follows:

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
- (a) for exercising the right of freedom of expression and information;
  - (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
  - (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
  - (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
  - (e) for the establishment, exercise or defense of legal claims.

**Under article 18 of GDPR data subjects may request restriction of processing of their personal data from the Controller as follows:**

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
- (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
  - (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
  - (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
  - (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

**Under article 21 of GDPR data subjects have the right to object against the processing of their personal data to the Controller as follows:**

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

**Under article 20 of GDPR data subjects have the right to portability of their personal data as follows:**

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
  - (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
  - (b) the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

**Under paragraph 2 of article 7 of GDPR data subjects have the right to withdraw their consent for processing their personal data at any time as follows:**

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

**The right of data subjects for remedy in court and to lodge complaints with a single supervisory authority**

If a data subject find out about unauthorized data processing he or she may initiate civil procedure against the Controller. This procedure falls within the scope of regional courts. The civil procedure – depending on the choice of the data subject – may be initiated at the regional court competent where he or she is domiciled (you can find the list and contact information of the regional courts via the following link: <http://birosag.hu/torvenyszekek>)

Without prejudice to other forms of administrative or court remedies every data subject is entitled to lodge complaints with a single supervisory authority – especially in the member state of residence, work place or where the suspected breach took place – if the data subject considers that the processing of his or her personal data is in violation of the GDPR.



**Hungarian National Authority for Data Protection and Freedom of Information  
(HNADPFI)**

address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c  
PO Box: 1530 Budapest, Pf.: 5  
e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)  
telephone: +36 (1) 391-1400  
fax.: +36 (1) 391-1410  
web: [www.naih.hu](http://www.naih.hu)

**Appendix to the Information leaflet about processing of personal data**

Purpose of processing	Categories of processed data	period for which the personal data will be processed	legal basis for the processing	Source of data	Recipient (if applicable)	Purpose of disclosure (if there is a recipient)
Processing of personal data of contact persons of the contracts in certain documents and electronic systems in order to prepare the contracts in accordance with the requirements of legal regulations. Recording, safekeeping, using and deleting of data in electronic database (contract management system).	Personal data: name, data of contact (phone number, email address) Sensitive data: none Data relating to children: none	The safekeeping time period of the document according to the subject of the contract.	Legal concern, to secure the operation of MVM XPERT Zrt.	Contracting party	none	none
Recording, safekeeping, using and deleting of data relating to fulfillment of contracts and registering related documents (minutes, technical documents, licensing documents from authorities, etc.)	Personal data: name, data of contact (phone number, email address) Sensitive data: none Data relating to children: none	The safekeeping time period of the document according to the subject of the contract.	Legal concern, to secure the operation of MVM XPERT Zrt.	Contracting party	Contracting party MVM Zrt. NÜSZ Zrt.	In accordance with the fulfillment of the contract
Recording, safekeeping, using and deleting of data relating to invoice management	Personal data: name, data of contact (phone number, email address) Sensitive data: none Data relating to children: none	Until the term of limitation of the document (normally 8 years after formation)	Legal concern, to secure the operation of MVM XPERT Zrt.	Contracting party	MVM Zrt. NÜSZ Zrt.	In order to manage invoices