Privacy Policy
On the processing of personal data with regard to the application of entry access and CCTV system upon entry to the area of MVM Paksi Atomerőmű Zrt.

Pursuant to Articles 13 and 14 of 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 (hereinafter: General Data Protection Regulation, GDPR), the Controller provides the following information to the data subjects regarding the processing of personal data.

	Controller	**Data Protection Officer**
Name:	MVM Paksi Atomerőmű Zrt.	István Kovács
Mailing address:	7031 Paks Pf. 71.	1031 Budapest, Szentendrei út 207-209
E-mail:	atomeromu@npp.hu	dpo@mvm.hu
Phone:	+36-75-505-000	+36-1-304-2000
Fax:	+36-1-355-1332	
Website	www.atomeromu.hu	
Registered office:	7030 Paks, Hrsz:8803/17.	

Legislative bases for data 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) (hereinafter: GDPR), the updated wording of the regulation is available through the following link: 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 the Right of Informational Self-determination and on Freedom of Information (hereinafter: Freedom of Information Act), the updated wording of the act is available through the following link: http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.338504)

According to the GDPR, **"personal data"**:
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.

*The definition of "**recipient**"*:
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.

File ID: FIB201_M04_V01.doc IBIR category: 2. For internal business use
Date of printing: 02 July 2018 07:50:07
This document is valid exclusively on the date of printing. Check validity prior to use.

PERSONAL DATA

purpose of processing #1:	Provision of the physical protection of MVM Paksi Atomerőmű Zrt. as required by the law, operation of the entry access system in order to provide access to the area, requests and registration of entry passes, granting authorisations, recording and use of data recorded during crossing entry points
purpose of processing #2:	Physical protection of MVM Paksi Atomerőmű Zrt. pursuant to legislative requirements, as well as the operation of closed-circuit television (CCTV) video surveillance system for the purposes of safety of life and asset protection (recording and use of images).
storage period #1:	During the term of validity of the entry pass, and 10 addition years after the expiry of validity.
storage period #2:	In the case of surveillance systems impacting public spaces 3 days after recording, in the case of surveillance systems only monitoring the facility, 60 days after the recording.
source:	Directly the data subject, data from authority control.

List of processed personal data:	**Why is the required?**
Personal identification data of natural persons	Legislative requirement, pursuant to the provisions of Act CXVI of 1996 and Government Decree 190/2011 (IX. 19.). Mandatory data.
Address	Legislative requirement, pursuant to the provisions of Act CXVI of 1996 and Government Decree 190/2011 (IX. 19.). Mandatory data.
Nationality	Legislative requirement, pursuant to the provisions of Act CXVI of 1996 and Government Decree 190/2011 (IX. 19.). Mandatory data.
Personal identity card or passport number	Legislative requirement, pursuant to the provisions of Act CXVI of 1996 and Government Decree 190/2011 (IX. 19.). Mandatory data.
Biometric identifier	Legislative requirement, pursuant to the provisions of Act CXVI of 1996 and Government Decree 190/2011 (IX. 19.). Mandatory data.
Number of public security authorisation issued by the police	Legislative requirement, pursuant to the provisions of Act CXVI of 1996 and Government Decree 190/2011 (IX. 19.).

	Mandatory data.
Payroll (entry card) number	Data mandatory for security purposes
Qualification, job position	Data mandatory for security purposes
Name of employer	Data mandatory for security purposes
Name of receiving organisation	Data mandatory for security purposes
Data of the entry system	Legislative requirement, pursuant to the provisions of Act CXVI of 1996, Government Decree 190/2011 (IX. 19.) and the physical protection plan, mandatory data.
Image, video	Legislative requirement, pursuant to the provisions of Act CXVI of 1996, Government Decree 190/2011 (IX. 19.) and the physical protection plan, mandatory data.
Vehicle registration (licence plate) number	Legislative requirement, pursuant to the provisions of Act CXVI of 1996 and Government Decree 190/2011 (IX. 19.). Mandatory data.

Legal ground for processing:	**Legislative requirement, Act CXVI of 1996, Act CLIX of 1997 and Government Decree 190/2011 (IX. 19.).**

List of recipients	**Purpose of disclosure**
MVM BSZK Zrt. 1117 Budapest, Budafoki út 54.	Data processor providing security services.
Atomix Kft. 7030 Paks, Hrsz.:8803/17.	Data processor providing security services.

Upon receiving the guest card and/or entering the real property, **you** (or in the case of persons under the age of 16, the holder of parental responsibility over the child)give consent**based on the Privacy Policy** to the processing of your above-specified personal data by the Controller, for the aforementioned purpose of processing (i.e. recording, organisation, storage, use, retrieval, transmission, safeguarding, deletion, destruction, preventing the re-use of the data).

The disclosure of personal data is subject to your decision, however in the lack of the above data we are unable to provide entry.

You may voluntarily withdraw your consent at any time, however the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Incomplete, contradictory or unintelligible indications shall be interpreted by the Controller as the denial of consent.
In the case of children under the age of 16 years, data processing of the child's personal data shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

WHO ARE AUTHORISED TO ACCESS YOUR PERSONAL DATA?

According to the principal rule, personal data of the data subject may only be disclosed with the employees of the Controller and the Data Processor designated by the Recipients, in the course of fulfiling their duties, including the provision of security services.

The Controller only discloses the personal data of the data subject with other government bodies in exceptional cases. This includes the case where judicial proceedings are initiated in the course of an on-going dispute between the data subject and the Controller, and the acting court of law finds it necessary to have the documents including the personal data of the data subject provided, or where the police contacts the Controller are requests the submission of documents including the personal data of the data subject for the investigation. Additionally, the attorney-at-law providing legal representation to the Controller can also access personal data in the case of a dispute between the data subject and the Controller.

DATA SECURITY MEASURES

The Controller stores the personal data provided by the data subject at the registered office or registered branch office of the Controller, and/or at the registered office or registered branch office of the Processor designated by the Recipients.

The Controller applies appropriate IT security measures to ensure that the personal data of the data subject are protected from e.g. unauthorised access or the unauthorised alteration thereof. For example, access to personal data stored on the servers is logged, which enables controlling at all time who accessed personal data, what personal data were affected and when the access has taken place. The Controller takes appropriate organisational measures to ensure the personal data are not made accessible to an indefinite number of natural persons.

Neither the Controller, nor the Data Processor transfers any personal data pursuant to this Privacy Policy to third parties or international organisations.

Neither the Controller, nor the Data Processor applies automated decision-making or profiling relevant to the personal data pursuant to this Privacy Policy.

YOUR RIGHTS

Pursuant to Article 15 of the GDPR, the data subject may request <u>access to the personal data</u> applicable to him or her, according to the following provisions:

(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 organisations;
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, 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) The Controller shall provide a copy of the personal data undergoing processing to the data subject. For any further copies requested by the data subject, the Controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

Pursuant to Article 16 of the GDPR, the data subject may request a rectification of inaccurate personal data applicable to him or her from the Controller.

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, *in the case of the data subject's such request.* 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.

Pursuant to Article 17 of the GDPR, the data subject may request the erasure of inaccurate personal data applicable to him or her from the Controller.

(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, and where there is no other legal ground for the processing;
c) the data subject objects to the processing in the public interest, in the exercise of official authority vested in the controller, or in the legitimate interest of the controller (third party), and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing in the interest of direct marketing purposes;
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 (*Hungarian law*) to which the controller is subject;
f) the personal data have been collected in relation to the offer of information society services.

(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.

File ID: FIB201_M04_V01.doc IBIR category: 2. For internal business use
Date of printing: 02 July 2018 07:50:07
This document is valid exclusively on the date of printing. Check validity prior to use.

(3) *The Data Subject's right to erasure may only be restricted* in the case of the following exceptions set forth in the GDPR, i.e. in case of the existence of the above reasons, the extended retention of the personal data is considered lawful:

a) for exercising the right of freedom of expression and information; or
b) for compliance with a legal obligation; or
c) for the performance of a task carried out in the public interest; or
d) in the exercise of official authority vested in the controller; or
e) for reasons of public interest in the area of public health;
f) for archiving purposes in the public interest; or
g) for scientific or historical research purposes or statistical purposes; or
h) for the establishment, exercise or defence of legal claims.

Pursuant to Article 18 of the GDPR, the data subject may request the restriction of processing personal data applicable to him or her from the Controller.

(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; or
d) the data subject has objected to the processing in the public interest, in the exercise of official authority vested in the controller, or in the legitimate interest of the controller (third party) 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.

Pursuant to Article 21 of the GDPR, the data subject may object the processing of personal data applicable to him or her from the Controller, according to the following provisions:

(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 the public interest, in the exercise of official authority vested in the controller, or in the legitimate interest of the controller (third party)*, including profiling based on those provisions. In such cases, 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. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

(3) At the latest at the time of the first communication with the data subject, the right to object shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

(4) 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.

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Pursuant to Article 20 of the GDPR, the data subject has right of the portability of the personal data applicable to him or her, according to the following provisions:

(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 legal ground for processing is the Data Subject's consent or the performance of a contract concluded with the Data Subject
b) and the processing is carried out by automated means.

(2) In exercising his or her right to data portability, 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 to portability shall be without prejudice to the right of erasure. The right to data portability 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 to data portability a copy shall not adversely affect the rights and freedoms of others.

Pursuant to Article 7 (3) of the GDPR, the data subject shall have the right to withdraw his or her consent to the processing of his or her personal data at any time, according to the following provisions:

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 data subject's right to seek remedy before a court of law, lodging a complaint with a supervisory authority

In the case of unlawful data processing experienced by the data subject, he or she may initiate a civil law lawsuit against the Controller. Such proceedings shall be adjudicated by the regional courts. Subject to the data subject's decision, the proceedings can be initiated at the regional court with jurisdiction over the data subject's address (see the list and contact data of regional courts http://birosag.hu/torvenyszekek
Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the GDPR.

Hungarian National Authority for Data Protection and Freedom of Information (NAIH)
address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
mailing address: 1530 Budapest, Pf.: 5
e-mail: ugyfelszolgalat@naih.hu
phone: +36 (1) 391-1400
fax: +36 (1) 391-1410
website: www.naih.hu