HM ARZENÁL Elektromechanikai ZRt.
Cím: 4461 Nyírtelek, Dózsa György út 121. Pf. 10.
Tel.: +36 (42) 210-555*, +36 (42) 210-801, Fax: +36 (42) 210-802
E-mail: info@hmarzenal.hu, Web: www.hmarzenal.hu
Cégjegyzékszám: 15-10-040092, cgj.v..bír.: Nyíregyházi Törvényszék

Data processing declaration

1. General provisions and contact details

This Data Processing Declaration (hereafter referred to as "the Declaration") refers to the processing of any information (hereinafter referred to as "Personal Information") processed by HM ARZENÁL Elektromechanikai ZRt. (Hereinafter referred to as the "Data Controller"), on any identified or identifiable natural person (hereinafter referred to as "the Data Subject").

The Data Controller shall keep data management legible and transparent, purposeful, economical, accurate, up-to-date and shall store data for a limited period of time safely and accountably, in accordance with Act CXII of 2011 on right of informational self-determination and Freedom of Information. (Act of Information.), and - from 2018/05 onwards - the Act No. 2016/679. (hereinafter referred to as the "GDPR").

1.1. Details of Data Controller

Name:	HM ARZENÁL Elektromechanikai Zrt.
Based:	4461 Nyírtelek, Dózsa György út 121.
Company reg. nr.:	15-10-040092
Tax nr.:	10753754-2-51
VAT reg. nr.:	HU10753754
Homepage:	www.hmarzenal.hu
Email address:	info@hmarzenal.hu
Data protection officer:	Szabó Dávdiné dr. Kovács Judit
Contact:	szabo.davidne@hmarzenal.hu +36-30-160-96-71

1.2. Availability and acceptance of the Declaration

Present Declaration and its amendments, if any, enter into force by its display on the homepage www.hmarzenal.hu .
By the disclosure of personal data, the Data Subject shall declare - at the time of display of present Declaration – he/ she was acquainted with the content of the version in force and explicitly accepts it. During the use of certain services, specific privacy terms may be applicable, whereabout the Data Controller gives preliminary information before the use of the service. Data Controller obtains the consent of each Data Subject, which is required to data processing, electronically (or inpaper version personally from the employées).

1.3. Definitions:

- „Personal Data” means any information concerning to the Data Subject; a natural person is identifiable, when directly or indirectly, in particularly by any identifier, for instance name, number, location data, online identification or by one or more features regarding the natural person’s psychical, physiological, genetic, intellectual, economic or cultural identity can be identified.
- „Processing of Personal Data” means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection,

recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

- „Data Controller" means the natural or legal person, public authority, agency or other body where the purposes and means of such processing of personal data are determined by European Union or Member State law (regarding this data processing declaration, it is the HM ARZENÁL Elektromechanikai ZRt.).
- „Data Processor" means a natural or legal person, public authority, agency or any entity, who processes personal data on behalf of Data Controller; (regarding this data processing declaration, an organisational entity or administrative employee of HM ARZENÁL Elektromechanikai ZRt.)
- „Recipient" means a natural or legal person, public authority, agency or another body, to whom or which the personal data are disclosed; those public authorities which may receive personal data in the framework of a particular inquiry in under the law of EU or a Member State 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, the purposes of the processing;
- „Consent" of the Data Subject means any freely given, specific, and unambiguous indication, which based on proper information, of the Data Subject's wishes, by which he/ she states or by a clear affirmative action he/ she indicates his/ her agreement to the processing of personal data relating to him/ her;
- „Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- „Data Protection Impact Assessment" means a type of processing - in particular using new technologies, - taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. Scope of processed data, law or purpose of data processing

According to this present Declaration, Data Controller performs data processing independently, and makes every effort to protect data security. Data base is stored on safe discs.
Data Controller forwards the personal data of Data Subject on a statutory ground to the data requesting authority, provided it has the appropriate legal basis.

2.1. The processing of the given data is performed by the voluntary, uninfluenced consent of the Data Subject for maintaining business connections, contracting, providing data as an owner and to the authorities. Data Contoller is not responsible for inaccurate or false data given by the Data Subject.

Purpose of processing and storage of personal data

- keeping contact with the Data Subject;
- identification of the Data Subject;
- testing and measuring of satisfaction of the Data Subject.

2.2. The processing of personal data of people employed as employees or in other contractual working relationships are performed in order to establish or maintain employment relationship. Data Controller is entitled on the basis of authorisation by law to perform data processing especially under the following legislation:

- Act I of 2012 on Labour Code
- Act LXXX of 1997 on Social Security
- Act XCIII of 1993 on Labour Safety

3. Data security provisions

Data Controller declares the appropriate security measures have been taken in order to protect personal data against unlawful access, alteration, forward, disclosure, deletion or destruction and unintended removal or damage, furthermore unavailability resulted from the change of applying technics. Data are stored using safe medium and and forwarded by safe channel in every case.
The Data Controller preserves electronically stored document and correspondence for 5 years. These are archived on file servers at workstations of data-processors, or on optical mediums at the administrative office.
Information Security Regulations contains rules to ensure security, under the standard ISO/IEC 27001:2013 which is annually audited internally and externally.
The fully comprehensive endpoint protection is provided by special security softwares.
The instructions in respect of the security of mobile devices are listed in the regarding normative measure of the CEO, together with the measures regarding the encrypted file system installed on devices.
The security of data and applications at the workstations are protected by user name, password, software firewall and hardware firewall.
Data Controller provides the security of data on servers, electronic correspondence, or security of computer network by user entitlements, special security softwares, hardware firewall or maintaining physically protected area.
Storage of optical data mediums is performed in a physically protected area and in a safe, which fulfill the requirements of security.

3.1. Rights to data protection and legal remedies of the Data Subject

Within the duration of data processing the Data Subject is entitled to:

- right to information,
- right to correction of data,
- right to deletion of data
- right to blocking the data, or
- right to object.

The Data Subject may request information about processing of personal data within the duration of data processing. The Data Controller within the shortest time, maximum a period of 25 days, from the date of submission of the application, informs the Data Subject intelligibly, in a written form on the data processed, the purpose, legal basis and duration of the data processing, and,- if the data is forwarded,- who and of what purpose received the data.
Furthermore, the Data Subject may request (a) the correction of his/ her personal data, with the exception mandatory data processing, (b) deletion or blocking of his/ her personal data. The Data Controller shall provide information at the regarding request of the Data Subject in written form, intelligibly within the shortest possible time from the submission of the request, but not later than within 25 days. If the Data Subject's request for correction, blocking or deletion is not completed by the Data Controller, within 25 days of receipt of the request, the Data Subject will be notified in a writtenform, or if he/ she agreed electronically, about the factual and legal justification of rejecting his/ her application for correction, blocking or deletion of the personal data.

The Data Subject may object against processing of his/ her personal data in cases specified in Act of information paragraph 21. §, if

- The processing or forwarding of personal data is necessary exclusively to fulfill the legal obligation of the Data Controller or to enforce the legitimate interest of Data Controller, Recipient or third party, with the exception of mandatory data processing and cases included in Act of information paragraph 6. § (5). (when personal data has been collected with the consent of the Data Subject and the Data Controller processes the data for the purpose of fulfilling his/her legal obligations.)
- the processing or forwarding of personal data – without the consent of the Data Subject – is performed for directmarketing, surveying or scientific research purposes.

The Data Controller shall examine the objection within the shortest time, but maximum within 25 days from the submission of the request, to make a decision on the merits of the case and shall inform the Data Subject in writing thereof.

3.2. If, according to the Data Subject the Data Controller has violated any legal provision on data processing or has failed to fulfill any requests, then in order to terminate the supposedly unlawful data processing, by a notification to the National Authority for Data Protection and Freedom of Information (http://naih.hu/; 1530 Budapest, Pf .: 5 telephone +36-1-391-1400: fax +36-1-391-1410: e-mail: ugyfelszolgalat@naih.hu) the Data Subject may initiate an investigation on the ground that personal data has been violated or immediate danger exists.

Beyond that, in case of violation of legal provisions on data processing, the Data Subject may also appeal to the competent judicial authority for legal remedy for which the Act of Information contains detailed rules.

4. Rights to Data protection and legal remedies

The primary rules for data protection rights and legal remedies of Data Subject have been included in the GDPR since 25 February 2018 (particularly in paragraphs 15-22, 77-79 and 82 and Chapter III of the GDPR preamble) The most important provisions are:

4.1. Access rights of the Data Subject:

The Data Subject is entitled to receive feedback from the Data Controller if his/ her personal data is being processed. If it is processed, he/ she is entitled to access his/ her personal information and the following information:
a) purpose of data processing;
b) categories of personal data of the Data Subject;
c) adressees or categories of addressees to whom the personal data are disclosed, including and in particularly the third country addressees or international organizations;
d) in the particular case, the intended duration of storing of personal data, if it is not possible, the criteria for determination of that period;
e) if data is not originated from the Data Subject, all the available information about their source;
f) information on the fact that decision-making is automated, including profiling, and its logic as well as information regarding the impacts of data processing on the Data Subject;
g) the Data Subject has the right to correct, delete his/ her personal data, limit the processing, object or make a complaint against the processing of his/ her personal data;
h) In cases, where personal data is forwarded to a third country, the Data Subject is entitled to receive information whether the data transfer have appropriate guarantees.

4.2. Right to correction and amendment

The Data Subject, on his/ her own request, is entitled to have the Data Controller specify, correct or amend his/ her incomplete personal data without undue delay.

4.3. Right to deletion ("right to forget notice")

The Data Subject, on his/ her request, is entitled to have his/her personal data deleted by the Data Controller without undue delay, if any of the following conditions exists:
a) personal data are no longer necessary for the initial purpose;
b) the Data Subject withdrew his/ her consent to data processing and the data processing has no other legal ground;
c) the Data Subject objects against data processing and in the particular case there is no priority legitimate reason for data processing;
d) the Data Controller processes personal data illegally;
e) the personal data shall be deleted to fulfill legal obligation.

If the Data Controller has disclosed personal data and it is required to delete under the paragraph above, Data Controller shall take reasonable steps, including technical measures, taking into consideration the available technology and implementation costs, in order to inform the other Data Controllers processing the data about the Data Subject verbal request to delete the links to personal data or the copy and replications of personal data.

The principles indicated above are not applicable if data processing is necessary:
a) in order to exercise the right to freedom of expression and information;
b) in order to fulfill any obligation by the law of the European Union or Member State concerning the processing of personal data applicable for Data Contoller;
c) for public archivation, or;
d) to submit, enforce or protect legal claims.

4.4. Right to the limitation of data processing

(1) The Data Subject, on his/ her own request, is entitled to have the Data Controller limit the processing of his/ her personal data to minimum level that is necessary, if any of the following conditions exists:
a) The Data Subject argues the accuracy of personal data, in this case limitation means the duration as long as it takes to ensure the accuracy of personal data;
b) The data processing is illegal but the Data Subject requests the limitation of data processing instead of deletion of data;
c) Personal Data are not required to be processed by the Data Controller, but the Data Subject requires them in order to submit, enforce or protect legal claims;
d) The Data Subject objected against data processing; (in this case, the limitation means the duration until it is determined whether the Data Controller's legitimate reasons have priority over the legitimate reasons of the Data Subject).

(2) If data processing is limited under paragraph one (1), such personal data may only be processed with the consent of the Data Subject or with the submission, enforcement or protection of legal claims of a natural or legal person, or in the important public interest of European Union or a Member State.
(3) The Data Controller shall prior inform the Data Subject about the removal of limitation of data processing.

4.5. Notification obligation in connection with correction or deletion of personal data or limitation of data processing.

The Data Controller shall inform all addressees about correction, deletion or limitation of data processing to whom Data Subject's personal data were provided, unless it is proven to be impossible or requires a disproportionately huge effort. The Data Subject, on his/ her request shall be informed about these addressees.

4.6 Right to data portability

(1) The Data Subject shall have the right to receive the personal data concerning him/ her, which he/ 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 or on a contract; and

b) the processing is carried out by automated means.

(2) In exercising his/ her right to data portability under paragraph one (1), the Data Subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

4.7. Right to object

(1) The Data Subject shall have the right to object, on grounds relating to his/ her particular situation, at any time to processing, including profiling, of his/ her personal data. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing, which have priority over the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.
(2) If personal data are processed for direct marketing purposes, the Data Subject shall have the right to object at any time to processing, Including profilig, of his/ her personal data for such marketing to the extent that it is related to such direct marketing.
(3) If the Data Subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
(4) In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the Data Subject may exercise his/ her right to object by automated means based on technical specifications.
(5) If personal data are processed for scientific or historical research purposes or statistical purposes, the Data Subject, on grounds relating to his/ her particular situation, shall have the right to object to processing of his/ her personal data, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

4.8. Right to make a complaint at the Supervisory Authority

The Data Subject is entitled to make a complaint against the Data Controller at the Supervisory Authority, when in his/ her opinion the processing of data violates the GDPR. The competent authority in Hungary is National Authority for Data Protection and Freedom of Information. (http://naih.hu/; 1530 Budapest, Pf.: 5.; telefon: +36-1-391-1400; fax: +36-1-391-1410; e-mail: ugyfelszolgalat@naih.hu).

4.9. Right to an effective judicial remedy against the supervisory authority

(1) The Data Subject shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority, which concerns him/ her.
(2) The Data Subject shall have the right to an effective judicial remedy, if a complaint was not handled by the supervisory authority or the Data Subject was not informed within three months on the progress or outcome of the complaint lodged.
(3) Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4.10. The right to effective judicial remedy against the Data Controller

(1) The Data Subject is entitled to an effective judicial remedy if in his/her opinion, his/ her rights under GDPR have been infringed as a result of the processing of his/ her personal data in non-compliance with GDPR.
(2) Proceedings against a controller shall be brought before the courts of the Member State where the Data Controller has an establishment or before the courts of the Member State where the Data Subject has his/ her habitual residence.

5. Procedure in case of data breach

If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the Data Subject without undue delay. The communication to the Data Subject shall describe in clear and plain language the nature of the personal data breach, the name and contact information of the Data Controller or another contact person, who can provide further information; also, it shall contain the probable consequences resulting from the data breach, furthermore, the implemented or planned measures by the Data Controller to remedy the data breach, including the measures to reduce the adverse consequences resulting from data breach. The Data Subject shall not be notified, if any of the following conditions exists:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise;
- giving information would involve disproportionate effort.

In such cases the Data Subject shall be informed by publicly disclosured information, or measures shall be taken, which ensure the similarly efficient communication to the Data Subjects. If the Data Subject has not been informed by the Data Controller about the data breach yet, the Supervisory Authority, after considering the probability of high risk, may impose providing the Data Subject with information.

The Data Controller, in accordance with the Article 55 of GDPR, shall report the data breach to National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C; telephone: (1) 391-1400; e-mail: ugyfelszolgalat@naih.hu) without undue delay, within 72 hours the latest, after the data protection officer was informed about the data breach, providing that the data breach will probably not constitute risk to the law and freedom of natural persons. If the notification is not completed within 72 hours, a notice to verify the reasons of delay shall be attached.

Clause:

The Data Controller considers this Declaration – with regard to its detailed content - as a data security regulation and in respect of which the Data Contoller undertakes to comply fully with its provisions.
Nyírtelek, 30. 04. 2018.

Made of: 1 copy
One copy: 8 sheets
Published:

- on the company webpage
- inner network

Original copy: archives