DATA PROCESSING AND PRIVACY POLICY

1. Introduction

Multimex Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság (registered address: 1037 Budapest, Erdőalja u. 147., company registry number: 01-09-260034, hereinafter referred to as "**Controller**") describes in the present data processing and privacy policy (hereinafter referred to as "**Policy**") how it collects, uses, transfers, forwards and stores the personal data of its customers. The Controller declares that this Policy complies with the data protection rules in force.

The Controller is entitled to unilaterally change the present Policy in order to make it comply with the law in force from time to time, including amendments related to changes in the Controller's services. Stakeholders are informed of any change of this Policy on the www.multimex.net website simultaneously with the change.

If you have any questions regarding this Policy, please write to us at the info@multimex.hu e-mail address. This Policy and all its amendments from time to time can be found on the www.multimex.net website.

In developing this Policy, the Controller considered the following legislation:

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing order line 95/46/EC (hereinafter referred to as "**GDPR**"),
- Act CXII of 2011 on the right of informational self-determination and freedom of information ("**Info Act**")
- Act V of 2013 on the Civil Code ("**Civil Code**")
- Act XLVIII of 2008 on the fundamental conditions and certain limitations of business advertising ("**BAA**"),
- Act CVIII of 2001 on certain issues concerning electronic commerce services and information society services ("**Etrade Act**")
- Act CXIX of 1995 on the processing of name and address data for the purpose of research and direct marketing ("**DM Act**")

- Act CXXXIII of 2005 on the rules of private security and private investigation activities ("**PS Act**")
- Act C of 2000 on accounting ("**Accounting Act**")
- Act CL of 2017 on the rules of taxation ("**Taxation Act**")
- Act CLV of 1997 on consumer protection ("**CP Act**")
- Act CLIX of 2012 on postal services ("**Postal Act**")
- Act CCXXXVII of 2013 on credit institutions and financial enterprises ("**Bank Act**");
- NGM Decree 19/2014. (IV. 29.) on the rules of procedure of the administration of guarantee and warranty claims regarding things sold under contracts between the consumers and undertakings ("**NGM Decree**");

2. Terms and definitions

When the following terms are used in this Policy, they have the following meanings:

'**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'**processing**' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'**restriction of processing**' means the marking of stored personal data with the aim of limiting their processing in the future;

'**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or national law, the controller or the specific criteria for its nomination may be provided for by Union or national law;

'**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.

'**pseudonymisation**' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

'**recipient**' means a natural or legal person, public authority, agency or any other body to which data are disclosed, whether a third party or not. 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;

'**cookie**' means a small text file which our web server sends to and reads back from the data subject's device (whether a computer, mobile telephone or tablet). There are temporary cookies (also known as session cookies) which are automatically deleted from your device when you close the browser, and there are longer-lasting cookies which remain on the device of the data subject for a long time (also depending on the settings of the device concerned);

'**data subject**' a natural person who is identified or directly or indirectly identifiable on the basis of personal data, who is always a specific person. Only natural persons are considered as data subjects, so legal entities are not and, thus, privacy protects the data of natural persons only. However, the data of private entrepreneurs or company representatives (e.g., telephone number, e-mail address, place and date of birth, etc.) are also considered as personal data.

'**data subject's consent**' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by clear affirmative action, signifies agreement to personal data relating to him or her being processed;

'**third party**' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who,

under the direct authority of the controller or processor, are authorised to process personal data;

'**third country**' means a country which is not a Member State of either the European Union or the European Economic Area. European Union Member States may enter into international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect any other provisions of the GDPR or European Union law;

'**binding corporate rules**' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

'**profiling**' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'**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. Natural persons may also be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them;

'**international organisation**' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

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

'**enterprise**' means a natural or legal person engaged in economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in economic activity.

3. Introduction of data processing principles

The Controller processes personal data lawfully, fairly and in a transparent manner in relation to the data subject, for clear and lawful purposes defined in this Policy and the documents annexed to it ('**according to the principle of purpose limitation**'). Processing is limited to what is necessary to achieve the objectives of the Controller ('**data minimisation**'). Under the principle of accuracy, the Controller ensures that the personal data it processes are up to date. To this end, the Controller takes all reasonable measures to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**principle of accuracy**'). The Controller acknowledges that personal data cannot be stored for longer than is necessary for the purposes for which the personal data are processed ('**principle of storage limitation**'). The Controller processes data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**'). The data security measures taken to comply with this processing principle are included in Section 9.8 of this Policy. The Controller keeps internal processing records on each processing operation to verify its conformity with the principles described ('**principle of accountability**').

The principles set out in this Policy describe our practices regarding personal data. Our processing principles apply to paper-based processing, as well as all devices, websites, customer service platforms or other online applications operated by the Controller, which refer to them through Internet reference or otherwise.

4. General information concerning data processing

The Controller processes the personal data of data subjects to provide the services used by the data subjects and improve the user experience of the data subjects. The Controller processes data involving personal data for the following purposes in relation to the activities listed below:

a) requests for quotation and information on the www.multimex.net website,
b) when ordering paper, products and services on the www.multimex.net website,
c) during the bug reports and when contacting with the Controller.

4.1. General information on the above processing:

a) **controller and its contacts: Multimex Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság** (registered address: 1037 Budapest, Erdőalja u. 147., company registry number: 01-09-260034, telephone: +(36) 1 481 4000, e-mail: info@multimex.hu, website: www.multimex.net);

b) **purpose and legal basis for the processing of personal data:** as defined below;

c) **period for which the personal data is stored or the criteria used to determine that period:** as defined below;

d) **data subjects** have the right defined in Section 8 of this Policy to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning them or to object to the processing as well as exercise the right to data portability.

The Controller has carried out or applies the interest balancing test in all cases in advance, takes into account the requirement of necessity and proportionality, the principle of gradualness and the requirement to give prior notice.

5. Scope of processed data. Purpose, duration and legal basis of processing. Persons with access to personal data and data transfer

5.1. Processing in the course of the orders given and the services provided on the www.multimex.net website:

- During the visit to the website, we are tracking the visitor anonymously by using, in particular, the Google Analytics and Google Search Console technology but do not use the data received for any purpose. Visiting information cannot be linked to a person.
- Requesting a quotation on the www.multimex.net website.
- Ordering products and services.
- Request for information.
- Reporting an issue, complaint handling.

5.2. Purpose of processing:

- Requests for quotations on the www.multimex.net website
- recording orders,
- performance of orders,
- issuing invoices,
- communication with the buyers,
- information to the buyers,
- customer service and complaint handling.

Providing your data is **voluntary.** You are not obliged to enter your personal data, but you cannot properly ask for a quotation or give orders (effectively reach our products and services) in their absence.

5.2. Duration of processing:

The duration of the cookies created by Google Analytics, Google Search Console, Facebook Pixel, Hot Jar is 30 days, while session IDs are automatically deleted when leaving the website.

Data provided by the user are erased by the controller within 10 working days of the user's written initiative. This claim can be notified to the info@multimex.hu e-mail address.

5.3. Legal grounds for data processing:

- In the case of a request for proposal and the sale of products and services, the consent of the data subject under paragraph a) of Section 5 (1) of the Info Act and paragraph a) of Article 6 (1) of the GDPR, as well as the performance of the contract under paragraph b) of Article 6 (1) of the GDPR;
- Performance of legal obligations during the documentation of purchase and payment, billing and arrangement of payment based on paragraph c) of Article 6 (1) of the GDPR, Section 169 (2) of the Accounting Act and Section 169 of the VAT Act;
- Identification of and communicating with the customer and during the performance of the ordered product (service): consent of the data subject under paragraph a) of Section 5 (1) of the Info Act, paragraph a) of Article 6 (1) of the GDPR, as well as the performance of the contract under paragraph b) of Article 6 (1) of the GDPR.

5.4. Persons with access to personal data

The data can be accessed by the staff of the Controller in order to carry out their functions.

5.5. Data transfer

Data is transferred to a third party or a recipient in the event that you were informed in advance of the potential recipient and then you consented in advance thereto, or it is otherwise required by law.

Your data will not be transferred to any third party other than under Section 5.4. Data is transferred to a third party or a recipient in the event that you were informed in advance of the potential recipient and then you consented in advance thereto, or it is otherwise required by law. In the course of this processing activity, personal data will not be transferred to third countries or international organizations.

6. Data security measures

The Controller must ensure the security of data and take all technical and organizational measures and establish the rules of procedure to ensure that the recorded, stored and processed data are protected, and prevent their destruction, unauthorized use or unauthorized alteration. It also calls on third parties to whom the data of the data subject are transferred to that they are required to meet the data security requirements.

The Controller ensures that no unauthorized person has access to, discloses, transmits, alters or deletes the processed data.

The Controller will do its utmost to ensure that the data are not accidentally damaged or destroyed. The Controller imposes the above commitment also on its employees involved in the processing activity and any data processors acting on behalf of the Controller.

In order to prevent unauthorized persons from accessing your data, the Controller ensures the protection of personal data and prevents unauthorized access as follows: access to the server and computers is protected by a password.

7. Notification of data subjects of a personal data breach

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.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller informs the data subject of the personal data breach without undue delay, using clear and plain language.

It is not necessary to inform the data subject if any of the following conditions are met:

a) 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;
b) the controller took subsequent measures following the personal data breach that ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialise;
c) providing the information would involve a disproportionate effort. In such a case, there must instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

8. Information on the rights of data subjects

8.1. Right to obtain information and right to access processed personal data:

The data subject has 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) purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipients 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.

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

The Controller shall provide a copy of the personal data undergoing processing. 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 Controller shall provide the information in a commonly used electronic form.

The right to obtain a copy referred to in the previous paragraph must not adversely affect the rights and freedoms of others.

The rights described above can be exercised through the contacts shown in Section 10.

8.2. Right to rectification:

The Controller will correct inaccurate personal information relevant to the data subject without undue delay at the request of the data subject. Taking into account the purpose of the processing, the data subject has the right to have his or her incomplete personal data

completed, including by means of providing a supplementary statement.

8.3. Right to erasure ("to be forgotten"):

If one or more of the following reasons prevail, the data subject may request the controller to erase personal data relating to him/her without undue delay if:

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 there is no other legal ground for the processing;
c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing or if the processing connects to direct marketing;
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.

Erasure of the data cannot be initiated if the 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 Data Controller is subject or for the performance of a task carried out in the public interest;
c) for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services based on Union or Member State law or pursuant to contract with a health professional and such data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or

Member State law or rules established by competent national bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by competent national bodies;

d) processing for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, based on Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

e) based on public interest in the area of public health, when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by competent national bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by competent national bodies;

f) for archiving in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

g) for the establishment, exercise or defence of legal claims.

8.4. Right to restriction of processing:

The Controller restricts processing at the request of the data subject where one of the following conditions applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the data subject 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 processing by the Controller based on public interest or legitimate interest, in this case, the restriction applies pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted under the above, such personal data shall, except for 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.

A data subject who has obtained restriction of processing having regard to the above will be informed by the controller before the restriction of processing is lifted.

8.5. Right to Data Portability:

The data subject has the right to receive the personal data concerning him or her, which he or she has provided to the Controller, in a structured, commonly used and machine-readable format and has 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 a contract; and
b) the processing is carried out by automated means.

In exercising his or her right to data portability as described above, the data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible.

Exercising the right to data portability may not violate the right to erasure (“to be forgotten”). 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.

The right to data portability must not adversely affect the rights and freedoms of others.

8.6. Right to object:

The data subject has the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her by the Controller where the legal basis of the processing is public interest or the implementation of duty for exercising public authority vested in the Controller, or is the need to pursue the legitimate interests of the Controller or a third party, including profiling based on the provisions referred to above. In this case, the Controller must 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.

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 must no longer be processed for such purposes.

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, has the right to object to the 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.

8.7. Right to withdrawal:

Where processing by the Controller is based on the consent of the data subject, the data subject has the right to withdraw the consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

8.8. Data security measures:

The Controller and the operator of the server network protect the data by applying the most advanced hardware and software support reasonably available against in particular unauthorized access, alteration, transfer, disclosure, erasure or destruction, as well as against accidental destruction or damage, thus serving data security. As a rule, the data processed by the Controller may be accessed only by the employees and other contributors of the Controller involved in the implementation of processing purposes defined in this Policy who are under the obligation of confidentiality with regard to all the data they come to know based on their employment contract or legal relationship applicable to their employment or other contractual relationship, statutory provisions or the Controller's instructions.

The Controller must accurately document all processing activities. The Controller must keep records of all processing activities carried out by it (e.g., newsletter, webshop, employee records). The Controller is keeping records of the transferred data to verify the legality of the data transfer and to provide information to the data subject, which records contain the transfer date of the personal data it processes, the legal basis and the recipient, the determination of the scope of the personal data transferred, and other data specified in the legislation on data processing.

8.9. Security of personal data processed on paper:

As a rule, the Controller does not process personal data on paper. When personal data are processed on paper, the Controller must immediately inform the data subject and apply the following rules:

- The data can be learned only by authorized persons, no other person can access them, nor may they be disclosed to any other person.
- The staff processing the data may leave the room where the processing takes place only after locking the data carriers assigned to them or locking the office.

- If personal data processed on paper are digitalised, the Controller applies the security rules governing documents stored digitally and demands the same from its processors as well.

8.10. Security of personal data stored digitally:

All access to the data is logged in a traceable manner.

Virus protection of the network processing personal data is continuously provided for.

Access to the network by unauthorized persons is prevented by the available computing devices and their use.

9. Rules on the notification of remarks, questions and complaints

Kindly send any questions or requests concerning your personal data stored in the system and processing to the info@multimex.hu e-mail address, or in writing to the 1037 Budapest, Erdőalja utca 147. address. Please keep in mind that, in your interest, we are able to provide information or take measures in relation to the processing of your personal data only if you demonstrate your identity satisfactorily.

Please be informed that data subjects may contact the Controller with regard to all issues related to the processing of their personal data and the exercise of their rights under the GDPR.

10. Legal redress

You can contact the Controller with any questions or comments related to the processing at any of the contacts shown in this Policy.

Legal remedies and complaints may also be submitted to the National Authority for Data Protection and Freedom of Information:

Name: Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information)
Office: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Postal address: 1530 Budapest, Pf.: 5.
Telephone: +36-1-391-1400
Fax: +36-1-391-1410
Website: www.naih.hu
E-mail: ugyfelszolgalat@naih.hu

In the event of any infringement of his or her rights, the data subject may file for court action against the Controller as the controller. The court hears such cases in priority proceedings. The Data Controller is required to demonstrate that the data control was in accordance with the law. Hearing such cases falls within the competence of the court of justice. If so requested by the data subject, the action may be brought before the court of justice in whose jurisdiction the data subject's home address or temporary residence is located.

The Controller is liable for any damage caused to a data subject as a result of unlawful processing of his or her data or by any breach of data security requirements. The data subject may claim restitution (Section 2:52 of the Civil Code) in the event of a violation of his or her rights to personality. The Controller is exempted from liability if the damage was caused by inevitable reasons beyond the scope of processing. The Controller will not reimburse the damage, and no restitution may be claimed from it to the extent that the damage occurred due to the wilful or grossly negligent conduct of the injured person.