PRIVACY NOTICE

Mito Group Zrt. (hereinafter: Data Controller) considers with the utmost of importance to respect the right of information self-determination of its partners and customers. The Data Controller processes personal data confidentially, in accordance with applicable European Union and domestic legislation, as well as with the relevant data protection (authority) practice, and takes all security and organizational measures that guarantee the security, confidentiality, integrity and availability of the data.

Considering the relevant provisions 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 (GDPR) and act CXII of 2011 on the right to information self-determination and freedom of information (hereinafter: Infotv.) Data Controller hereby publishes the following privacy notice (hereinafter: Privacy Notice) for the protection of personal data.

The present Privacy Notice is effective from 2023.03.16. until withdrawn, in relation to the processing of the personal data of those involved in the activities carried out by the Data Controller.

The Data Controller reserves the right to unilaterally amend this Privacy Notice at any time. If the present Privacy Notice is amended, the Data Controller will inform the data subjects accordingly.

SUBJECT OF DATA PROCESSING

Based on your prior, clear and express consent, the Data Controller sends newsletters to the data subject in the form of e-mail with a collection of articles on the recent news and curiosities of the advertising industry.

The data subject can subscribe to the newsletter in electronic form on the website of the Data Controller, http://mito.hu/weekly the condition for which is to read the present Privacy Notice.

The Data Controller does not take responsibility in any form for errors or damages resulting from erroneously or falsely provided data, the Subscriber bears all kinds of responsibility resulting from this. The Data Controller is obliged to delete subscriptions provided with incorrect or false data immediately after becoming aware of them.
The Data Controller ensures that the data subject can unsubscribe from the newsletters free of charge at any time.

The Data Controller processes personal data as follows:

Scope of processed personal data: full name and email address

Categories of data subjects: data subjects who subscribe to the newsletter.

Source of processed personal data: the data subject.

Purpose of data management: newsletter sending.

Legal basis for data management: the consent of the data subject based on Article 6 (1) point a) of the GDPR.
In the course of asserting a right or claim, as well as in the processing of contact data, based on point f) of Article 6 (1) of the GDPR, the legal basis is the legitimate interest of the Data Controller.

Duration of data processing: after the assessment of the declaration (unsubscribing request) sent by the data subject or its representative to the Data Controller to delete its personal data - if the request is justified - the data subject's personal data will be deleted immediately and irretrievably. An exception to this is the possible enforcement of rights or claims, by court, prosecutor's office, investigative authority, violation authority, public administrative authority, the National Authority for Data Protection and Freedom of Information, or others authorized by law.

Access: the Data Controller primarily has access to the processed personal data.

Data transfer: personal data will only be forwarded to the listed data processors, or the possible enforcement of rights or claims, by court, prosecutor's office, investigative authority, violation authority, public administrative authority, the National Authority for Data Protection and Freedom of Information, or others authorized by law.

The technique of data processing: The Data Controller processes the data subject's personal data electronically.

Profiling: the Data Controller does not make a decision based solely on automated data management in connection with the data subject, nor does it to create a profile of the data subject based on the available personal data.

Data subject rights: in connection with data management, data subjects may exercise their rights to withdraw consent, access, rectification, deletion, restriction of data processing, and data portability.

DATA PROCESSOR

Company:	**Mailgun Technologies, Inc., a Delaware corporation**
Registered Office:	251 LITTLE FALLS DRIVE, WILMINGTON, New Castle, DE, 19808
Company reg. no.:	6297323
Privacy Policy:	https://www.mailjet.com/legal/privacy-policy/
Activity:	data storage, compilation of newsletters, monitoring, compilation of statistics

RIGHTS OF DATA SUBJECT

Corresponding to applicable data protection laws, you – based on the given circumstances – shall have the:

a) right to request access to your personal data;
b) right to have your personal data rectified;
c) right to have your personal data erased;
d) right to restrict the processing of your personal data;
e) withdraw the consent provided to the processing of personal data.
f) d) the right to data portability, if the conditions specified in the legislation exist, and
g) e) in the case of data processing based on legitimate interest, the right to protest.

Right of access:

The data subject has the right to receive feedback from the data controller as to whether his personal data is being processed, and if such data processing is underway, he is entitled to receive access to the personal data. The Data Controller provides the Data Subject with a copy of the personal data that is the subject of data processing. For additional copies requested by the Data Subject, the Data Controller may charge a reasonable fee based on administrative costs. If the Data Subject submitted the request electronically, the information must be provided in a widely used electronic format, unless the Data Subject requests otherwise.

Right to rectification:

The Data Subject has the right to have inaccurate personal data corrected without undue delay upon request by the Data Controller.

Right to erasure:

The data subject has the right to have the data controller delete the personal data concerning him without undue delay at his request, and the data controller is obliged to delete the personal data concerning the data subject without undue delay if one of the following reasons exists:

a) the personal data are no longer needed for the purpose for which they were collected or otherwise processed;

b) the data subject withdraws the consent that forms the basis of the data management pursuant to point a) of Article 6 (1) or point a) of Article 9 (2) of the General Data Protection Regulation, and there is no other legal basis for the data management;

c) the Data Subject objects to the data processing based on Article 21 (1) of the General Data Protection Regulation and there is no overriding legitimate reason for the data management,

or the Data Subject objects to the data management based on Article 21 (2) of the General Data Protection Regulation;

d) personal data were handled unlawfully;

e) personal data must be deleted in order to fulfill the legal obligation prescribed by EU or Member State law applicable to the Data Controller;

f) the collection of personal data took place in connection with the offer of information society-related services referred to in Article 8 (1) of the General Data Protection Regulation (conditions for the consent of children).

Right to restrict data processing:

The Data Subject is entitled to request that the Data Controller to restrict data processing if one of the following conditions is met:
a) the data subject disputes the accuracy of the personal data, in which case the limitation applies to the period that allows the data controller to check the accuracy of the personal data;

b) the data management is unlawful and the data subject opposes the deletion of the data and instead requests the restriction of their use;

c) the data controller no longer needs the personal data for the purpose of data management, but the data subject requires them to submit, enforce or defend legal claims; or

d) the data subject has objected to data processing in accordance with Article 21 (1) of the General Data Protection Regulation; in this case, the restriction applies to the period until it is determined whether the legitimate reasons of the data controller take precedence over the legitimate reasons of the data subject.

If data processing is subject to restrictions, such personal data may only be processed with the consent of the Data Subject, except for storage, or to submit, enforce or defend legal claims, or to protect the rights of another natural or legal person, or in the important public interest of the European Union or a member state.

Right to data portability:

The Data Subject is also entitled to receive the personal data relating to him provided to the Data Controller in a segmented, widely used, machine-readable format, and is also entitled to transmit this data to another data controller without being hindered by the data controller, to which the personal data has been made available, if: (i) the data processing is based on consent according to point a) of Article 6 (1) of the General Data Protection Regulation or point a) of Article 9 (2) of the General Data Protection Regulation, or on a contract according to Article 6 (1) point a) of the General Data Protection Regulation and (ii) data management is performed in an automated manner.

Right to protest:

The Data Subject has the right to object at any time to the processing of his personal data based on points e) or f) of Article 6 (1), including profiling based on the aforementioned provisions, at any time for reasons related to his own situation. In this case, the data controller may no longer process the personal data, unless the Data Controller proves that the data processing is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or that are necessary for the presentation, enforcement or defense of legal claims are connected.

General rules for the exercise of the rights of the data subjects:

The Data Controller shall inform the Data Subject without undue delay, but no later than one month from the receipt of the request, of the measures taken as a result of the request. If necessary, taking into account the complexity of the application and the number of applications, this deadline can be extended by another two months. The Data Controller shall inform the Data Subject of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request. If the Data Subject submitted the request electronically, the information must be provided electronically, if possible, unless the Data Subject requests otherwise.
The Data Controller provides the Data Subject with information and measures free of charge. If the Data Subject's request is clearly unfounded or - especially due to its repetitive nature - excessive, the Data Controller, taking into account the administrative costs associated with providing the requested information or information or taking the requested action:

a) may charge a fee of a reasonable amount, or

b) may refuse to take action based on the request.

It is the responsibility of the Data Controller to prove that the request is clearly unfounded or excessive.

If the Data Controller has reasonable doubts about the identity of the natural person who submitted the request, it may request the provision of additional information necessary to confirm the Data Subject's identity.

DATA SECURITY

The Data Controller and the data processor are entitled to access the personal data of the data subject only to the extent necessary for the performance of their tasks.

In order to ensure data security, the Data Controller assesses and records all data management activities carried out by it.

Based on the records of data management activities, the Data Controller performs a risk analysis in order to assess the conditions under which each data management is carried out,

as well as which risk factors during data management may cause harm and possible data protection incidents. The risk analysis must be performed on the basis of the actual data management activity. The purpose of the risk analysis is to define security rules and measures that, in line with the performance of the Data Controller's activities, effectively ensure the adequate protection of personal data.

Taking into account the nature, scope, circumstances and purposes of data processing, as well as the varying probability and severity of the risk to the rights and freedoms of natural persons, the Data Controller implements appropriate technical and organizational measures in order to ensure and prove that the processing of personal data is in accordance with GDPR. Including, but not limited to, where appropriate:
- pseudonymization and encryption of personal data;
- ensuring the continuous confidentiality, integrity, availability and resilience of the systems and services used to manage personal data;
- in the event of a physical or technical incident, the ability to restore access to personal data and the availability of data in a timely manner;
- a procedure for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures taken to guarantee the security of data management.

When determining the appropriate level of security, it is necessary to specifically take into account the risks arising from data processing, which in particular arise from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise managed.

The Data Controller implements appropriate technical and organizational measures to ensure that, by default, only such personal data is processed that is necessary for the given specific data management purpose. This obligation applies to the amount of personal data collected, the extent of their processing, the duration of their storage and their accessibility. In particular, these measures must ensure that personal data cannot by default become accessible to an indefinite number of persons without the intervention of the natural person. In case of damage or destruction of personal data, attempts must be made to replace the damaged data from other available data sources to the extent possible. The fact of the replacement must be indicated on the replaced data.

The Data Controller protects its internal network with multi-level firewall protection. A hardware firewall (border protection device) is always located at the entry points of the used public networks. The Data Controller stores the data redundantly - i.e. in several places - to protect them from destruction, loss, damage, and unlawful destruction resulting from the failure of the IT device.

It protects internal networks from external attacks with multi-level, active, complex protection against malicious codes (e.g. virus protection).

The Data Controller does everything with the utmost care that can be expected of him to ensure that his IT tools and software continuously comply with the technological solutions generally accepted in market operation.

LEGAL REMEDIES

The Data Subject may at any time contact the Data Controller at adatvedelem@mito.hu.

In the event of a violation of their rights, the Data Subject may apply to court against the Data Controller. The court acts out of sequence in the case. The Data Controller is obliged to prove that the data management complies with the provisions of the law. The adjudication of the lawsuit falls within the jurisdiction of the court, in the capital, the Metropolitan Court. The lawsuit can also be initiated before the court of residence or residence of the Data Subject.

The Data Controller is obliged to compensate the damage caused to others by the unlawful handling of the Data Subject's data or by violating the requirements of data security. The Data Controller is released from liability if it proves that the damage was caused by an unavoidable cause outside the scope of data management. There is no need to compensate the damage if it resulted from the intentional or grossly negligent behavior of the injured party.

In the event of a complaint regarding the handling of his personal data, the Data Subject may also contact the National Authority for Data Protection and Freedom of Information (dr. Attila Péterfalvi, President of the National Authority for Data Protection and Freedom of Information, postal address: 1530 Budapest, Pf.: 5., address: 1125 Budapest, Erzsébet Szilágyi fasor 22/c, Phone: +36 (1) 391-1400; Fax: +36 (1) 391-1410; E-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu).