FLONO Kereskedelmi és Szolgáltató Kft.
data management policy

FLONO Kereskedelmi és Szolgáltató Kft. (Registered office: 3742 Rudolftelep, József Attila utca 5; company registration number: 05 09 031949; tax number: 24883782205; company gate: 24883782 .; hereinafter: the **Data Controller** or **the Company)** in order to fully comply with the legal provisions in force, the present as data management (hereinafter: **the Regulations) .** The Regulations can be viewed at the Data Controller's headquarters and on the website (https://www.flono.hu).

The data controller shall comply with the personal data and information provided by the clients in full compliance with the applicable European Union and Hungarian data protection legislation (in particular Act CXII of 2011 on the right to information self-determination and freedom of information, Act LXXVIII of 2017 on legal activities) and other applicable legislation. treated in accordance with the When drafting the provisions of the Regulations, the Data Controller took special account having regard to Decision 2016/679 of the European Parliament and of the Council s. Regulation (hereinafter: **General Data Protection Regulation** or **GDPR) .**

Visitors to the Data Controller's website (https://www.flono.hu) or who come into contact with the Data Controller in any way, as well as any obligations following the contact on issues related to the processing of personal data of a person establishing a legal relationship (hereinafter: **Legal Relationship)** (hereinafter: **Customer) ,** such as the *facts related to* the processing of data, the *purpose, legal basis, duration of* data processing, the *scope of persons entitled to access* personal data and the *processing* of data This Regulation provides information before These Rules also cover the Customer's *rights* and *remedies in* relation to data processing . The Data Controller emphasizes that the stored data is stored securely, and upon its request, the Customer shall provide information about the stored data and the Customer may request the deletion of the data at any time, free of charge and without justification, unless required by law.

1.) DATA OF **THE DATA CONTROLLER**

The data controller is **FLONO Kereskedelmi és Szolgáltató Kft.**

Headquarter:	3742 Rudolftelep, József Attila utca 5.
Registry court:	Miskolc Court of Justice
Company registration number:	05 09 031949
Tax number:	24883782205
His e-mail address:	additive@flono.hu
Phone number:	+36202624489

2.) RELEVANT RULES

The data controller undertakes to carry out its activities in accordance with the legislation in force at any time. At the time of the adoption of these Regulations, these include, but are not limited to:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46

- 2011 CXII. Act on the Right to Information Self-Determination and Freedom of Information. Act C of 2000 on Accounting
-

3.) CONCEPTS

2011 CXII. Pursuant to Section 3 of the Act on the Right to Self-Determination of Information and Freedom of Information:

1. *Data subject:* identified or directly identified on the basis of any specific personal data or indirectly, an identifiable natural person;
2. *Personal data: data* which can be contacted with the data subject, in particular the name of the data subject, his or her identification mark and knowledge of one or more physical, physiological, mental, economic, cultural or social identity from the data, inference that can be
3. *Consent:* the voluntary and explicit expression of the will of the data subject, based on adequate information and giving his or her unambiguous consent to the processing of personal data concerning him or her, in full or in part;
4. *Objection:* a statement by the data subject objecting to the processing of his or her personal data and the requests the termination of data processing or the deletion of processed data;
5. *Data controller:* a natural or legal person, or an organization without legal personality, which alone or jointly with others determines the purpose of data processing, makes and implements decisions on data processing (including the means used), or with a data controller entrusted by it. executes;
6. *Data management:* any operation or set of operations on data, regardless of the procedure used, in particular the collection, recording, recording, systematisation, storage, modification, use, interrogation, transmission, reconciliation or linking, blocking, erasure and destruction of data , and to prevent the further use of data, the taking of photographs, sound or images and the recording of physical characteristics capable of identifying a person;
7. *Data transfer:* the data is made available to a specific third party making;
8. *Disclosure: making* the data available to anyone;
9. *Data erasure:* making data unrecognizable in such a way that it is no longer recovered not possible;
10. Data marking: the identification of the data in order to distinguish it;
11. *Data blocking:* the identification of the data for further processing is final or for a limited period of time;
12. *Destruction of data:* complete physical destruction of the data carrier;
13. *Data processing:* the performance of technical tasks related to data management operations, regardless of the method and means used to perform the operations and the place of application, provided that the technical task is performed on the data;
14. *Data processor:* a natural or legal person or an organization without legal personality who, under a contract concluded with a data controller, including the conclusion of a contract pursuant to a legal provision - processes data;
15. *Data controller:* the body performing a public task which has produced data of public interest to be published compulsorily by electronic means, or in the course of the operation of which this data has been generated;
16. *Informant:* a body performing a public task which, if the data controller does not publish the data itself, publishes the data provided to it by the data controller on a website;
17. *Data set:* the totality of the data managed in one register;

18. *Third party:* any natural or legal person, or any entity without legal personality, other than the data subject, the controller or the processor;

19. *EEA State:* a Member State of the European Union and another State party to the Agreement on the European Economic Area, as well as a State of which the European Union and its Member States and a State not party to the Agreement on the European Economic Area is a national. Enjoys the same status as a national of a State party to the Agreement on the European Economic Area;

Third country: any state that is not an EEA state.

4.) PRINCIPLES OF DATA MANAGEMENT

- The data subject *consents* (Article 6 (1) (a) of the GDPR)
- Necessary for *the performance of the contract ,* (GDPR Article 6 (1) (b)) or
- It is ordered by *law* or - by the authority of law, within the scope specified therein - by a decree of a local government. (Article 6 (1) (c) of the GDPR).

The declaration of an incapacitated and incapacitated minor requires the consent of his or her legal representative, except for those parts of the service where the declaration is intended for mass registration in everyday life and does not require special consideration.

Personal and special data may only be processed for a specific purpose, in order to exercise a right and fulfill an obligation. This purpose must be met at all stages of data management.

Only personal data that is necessary for the realization of the purpose of data processing and is suitable for the achievement of the purpose may be processed only to the extent and for the time necessary for the realization of the purpose.

Personal data may only be processed with informed consent.

The customer shall be informed in a clear, comprehensible and detailed manner of all facts relating to the processing of his data, in particular the purpose and legal basis of the processing, the person authorized to process and process the data, the duration of the processing and who may have access to the data. The information must also cover the Customer's data management rights and remedies.

The personal data processed must meet the following requirements:

- Their admission and treatment is fair and lawful;
- Accurate, complete and timely when needed;
- The manner in which they are stored is such that the data subject can be identified only for the time necessary for the purpose of storage. The use of a general and unique identification mark is prohibited.
-

Personal data may be transferred and the various data processing operations may be combined if the data subject has consented to it or is permitted by law and if the conditions for data processing are met for each personal data.
Personal data from Hungary - regardless of the data carrier or the method of data transfer - to a controller or processor in a third country if the Customer has expressly consented to it or is permitted by law and in the third country

An adequate level of protection of personal data is ensured during the handling and processing of the transferred data. The transfer of data to the EEA States shall be deemed to take place within the territory of Hungary.

5.) PERSONAL AND SPECIAL DATA PROCESSED BY THE DATA CONTROLLER, THEIR SOURCES, PURPOSE, LEGAL BASIS AND DURATION OF THE DATA PROCESSING:

Data	Data source	Purpose of data management	Legal basis for data management	Duration of data management
name	Customer	(a) contact (b) invitation to tender (c) the conclusion of a contract (d) performance of a contract e) invoicing	-contribution concerned (Article 6 (1a) GDPR): (a) for objectives (b) (Article 6 (1b) (c) (d) (e) of the GDPR) objectives	-to the request for erasure: a) b) objectives -for 5 years after the performance of the contract (limitation according to period of the Civil Code): c) d) objectives For 8 years specified in the Accounting Act: e) in the case of a target
e-mail address	Customer	(a) invitation to tender b) contact (c) the conclusion of a contract (d) performance of a contract e) communication	-contribution concerned (Article 6 (1a) GDPR) for the purposes of: (a) (b) (e) performance of the contract (Article 6 (1b) of the GDPR): c) d) e) objectives	-to a request for erasure: a) for purposes of b) purposes e) 5 years after the performance of the contract (according to the Civil Code limitation period): for purposes of c) d) e)
phone number	Customer	(a) contact b) contact (c) the conclusion of a contract (d) performance of a contract	-affected consent (Article 6 (1a) GDPR: a) b) c) d) objectives -performance of the contract (Article 6 (1b) GDPR): c) d) objectives	-to the request for erasure: a) b) objectives 5 years after the performance of the contract (statute of limitations according to

			in the case of	deadline): (c) for purposes (d)
Home address	Customer	(a) the conclusion of a contract (b) performance of a contract c) invoicing	-performance of the contract (Article 6 (1b) of the GDPR): for purposes of (a) (b) -fulfillment of a legal obligation (Article 6 (1c) GDPR: in case of objective c)	-contract according to for 5 years after the fulfillment of the Civil Code (limitation period of the Civil Code): a) b) objectives For 8 years specified in the Accounting Act: c) for the purpose
bank account details (name of the bank holding the account, bank account number)	Customer	(a) the conclusion of a contract (b) performance of a contract c) invoicing (d) payment for a service	performance of the contract (Article 6 of the GDPR) 1b): for purposes a) b) c) d)	5 years after the performance of the contract (limitation according to period of the Civil Code): a) b) d) for purposes For 8 years specified in the Accounting Act: c) for the purpose

The Data Controller and the data processors used by him / her are entitled to access personal and special data in accordance with the applicable legislation.

Cookie: This website uses cookies. A cookie that is sent by a web server has a an alphanumeric information packet that is recorded on Customer's computer and stored for a predetermined period of validity. The purpose of the cookie is to ensure the proper functioning of the website, the basic and convenience functions, and to increase the security of the website, to improve the website and to generate traffic statistics. The use of cookies is only permitted if it is permitted by the Client's browser.

Enabling depends on the configuration of the Client's browser. The Customer is the website by opening it, you consent to the use of cookies.

6.) DATA PROCESSORS, ENTITLED TO ACCESS PERSONAL DATA

The Data Controller and the data processors used by him / her are entitled to access personal data in accordance with the applicable legislation.

The processing of data is performed by the following data processors acting on behalf of the Data Controller:

Gusztáv Litkai as an accountant
Headquarters: 2119, Pécel Boncsok utca 36.

Type of data transmitted: Customer's name, address, bank account data.
The purpose of data processing is to perform accounting tasks in particular, but not exclusively, in accordance with the provisions of the Law on Taxation and Accounting, using data specified in the applicable legislation.

WIX Ltd. as a hosting provider
Head office: 40 Namal, Tel Aviv Street, Tel Aviv L3 6701101 Israel
Business Registration Number: 98-0685109 (USA)
Tax number: EU442008451

Type of data transmitted: Customer name, e-mail address
Purpose of data management: operation of the messaging system on the Company's Website

The data controller reserves the right to involve an additional data processor in the future data management, of which it informs the Client by amending these Regulations.
Unless expressly provided by law, the Data Controller shall only transfer personally identifiable data to third parties with the express consent of the Customer, excluding the transfer of data necessary for the performance of the services provided by the Data Controller to the Data Controller's contractual partners.

7.) CUSTOMER'S RIGHTS

The Customer may request from the Data Controller to provide information on the handling of his / her personal data, to request the correction of his / her personal data, and to request the deletion or blocking of his / her personal data, except for mandatory data processing.
The Customer may request from the Data Controller access to, rectification, deletion or restriction of the processing of personal data concerning him / her - if its registration, storage, preservation or transmission is not required by law. In addition, you have the right to receive your personal data provided to you by the Data Controller in a structured, widely used machine-readable format and to transfer this data to another data controller (right to data portability). The data subject shall also have the right to withdraw his or her consent to the processing at any time, without prejudice to the lawfulness of the data processing prior to the withdrawal.

Below is a brief description of each of the data subject's rights:

Access to personal and special data

At the request of the Customer, the Data Controller shall provide information on whether the Data Controller conducts data processing regarding his / her personal and special data and, if so, shall grant him / her access to the personal and special data and inform him / her of the following information:

- purpose (s) of data processing;
- the types of personal and / or special data involved in the processing;
in the case of the transfer of the Customer 's personal data, the legal basis for the transfer, and consignee (s);

- the planned duration of the data processing;
- the Customer's rights in connection with the rectification, deletion and restriction of the processing of personal data and the protest against the processing of personal data;
- the possibility of recourse to the Authority;
- source of data;
- the names and addresses of the data processors and their activities related to data processing.

The Data Controller shall provide the Customer with a copy of the personal and special data subject to data processing free of charge. For additional copies requested by the Customer, the Data Controller may charge a reasonable fee based on administrative costs. If the Customer has submitted the request electronically, the information shall be provided in a widely used electronic format, unless otherwise requested by the data subject.

The data controller is obliged to provide the information at the request of the Customer in an intelligible form without undue delay, but no later than within one month from the submission of the request.
The Customer may submit a request for access at the contact details specified in point *1)* .

Correction of managed data

The Customer may request from the Data Controller (at the contact details specified in point 1) the correction of inaccurate personal data or the supplementation of incomplete data, taking into account the purpose of the data processing. The data controller shall carry out the correction without undue delay.

Delete managed data (right to forget), lock
The Customer may request that the Data Controller delete personal or special data concerning him / her without undue delay, and the Data Controller shall delete the personal or special data concerning the Customer without undue delay if any of the following reasons exists:

(a) personal data are no longer required for the purpose for which they were collected or otherwise processed;
b) the Customer withdraws his consent and there is no other legal basis for the data processing;
c) the Customer objects to the processing of his / her personal data;
(d) personal data have been processed unlawfully;
(e) personal data must be deleted in order to fulfill a legal obligation to which the controller is subject under applicable Union or Member State law;
(f) personal data have been collected in connection with the provision of information society services to children.

If the Data Controller has disclosed (made available to a third party) personal data and is obliged to delete it in accordance with the above, it shall take reasonable steps, taking into account the available technology and the costs of implementation, to take measures to inform the personal data concerned. data controllers that the Customer has requested the deletion of links to the personal data in question or of a copy or duplicate of such personal data.

Personal or special data need not be deleted if the processing is necessary:

- to exercise the right to freedom of expression and information;

- EU or Member State law governing the processing of personal data
  for the performance of a legal obligation or for the performance of a task performed in the public interest or in the exercise of a public authority delegated to the Data Controller;
- on grounds of public interest in the field of public health;
- for archiving purposes in the public interest, for scientific and historical research purposes or for statistical purposes, where the right of erasure would be likely to make such processing impossible or seriously jeopardize; obsession
- to submit, enforce or defend legal claims.

Restrict managed data

The Customer is entitled to restrict the data processing at the request of the Data Controller instead of correcting or deleting the personal data if any of the following is met:

- the Customer disputes the accuracy of the personal data, in which case the restriction applies to the period of time that allows the Data Controller to check the accuracy of the personal data;

- the data processing is illegal and the Customer objects to the deletion of the data and requests it instead restrictions on the use of
- the Data Controller no longer needs the personal data for the purpose of data processing, but the Customer requests them in order to submit, enforce or protect legal claims;

  obsession
- the Customer objected to the data processing; in this case, the restriction shall apply for 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 the processing is subject to restrictions, such personal data may be processed, with the exception of storage, only with the consent of the Customer or for the purpose of bringing, enforcing or protecting legal claims or protecting the rights of another natural or legal person or in the important public interest of the Union or a Member State.

The Data Controller shall inform the Customer, at whose request the data processing has been restricted, in advance of the lifting of the data processing restriction.

Obligation to notify the rectification or erasure of personal data or the restriction of data processing

The Data Controller shall inform all recipients to whom or with whom the personal data have been communicated of the rectification, erasure or restriction of the processing of personal data, unless this proves impossible or requires a disproportionate effort. Upon request, the Data Controller shall inform the Customer of these recipients.

Right to protest

The Customer may object to the processing of his / her personal data if the processing of the data:

- necessary for the performance of a task in the public interest or in the exercise of a public authority conferred on the Data Controller;
- necessary for the legitimate interests of the Data Controller or a third party;
- based on profiling.

In the event of the Customer's objection, the Data Controller may not further process the personal data, unless it proves that the data processing is justified by compelling legitimate reasons that take precedence over the Customer's interests, rights and freedoms or related to the submission, enforcement or protection of legal claims. .
If personal data is processed for the purpose of direct business acquisition or related profiling, the Customer has the right to object at any time to the processing of personal data relating to him for this purpose. If the Customer objects to the processing of personal data for the purpose of direct business acquisition, the personal data may no longer be processed for this purpose.

The Data Controller shall, without undue delay, but no later than **30 days from** the receipt of the request , inform the Customer of the measures taken following the request for *access, rectification, deletion, restriction, protest* and *data portability .* If necessary, taking into account the complexity of the application and the number of applications, this period may be extended by a **further two months. The Data Controller shall inform the Customer about the extension of the deadline within 30 days from** the receipt of the request, indicating the reasons for the delay . If the Customer has submitted the request electronically, the information shall, if possible, be provided electronically, unless otherwise requested by the data subject.

If the Data Controller fails to take action at the request of the Customer, **it shall inform the Customer without delay, but no later than within one month from the receipt of the request, of the reasons for non** -compliance and that the Customer may lodge a complaint with a supervisory authority.

Upon the Customer's request, the information, information and action taken on the Customer's request shall be provided free of charge. If the Customer's request is manifestly unfounded or, in particular due to its repetitive nature, excessive, the Data Controller may charge a reasonable fee or refuse to act on the request, taking into account the administrative costs of providing the requested information or action or taking the requested action. The burden of proving that the request is manifestly unfounded or excessive is on the Data Controller.

8.) DATA SECURITY

The Data Controller undertakes to ensure the security of the data, to take the technical and organizational measures and to establish the procedural rules to ensure that the recorded, stored and processed data are protected and to prevent
their destruction, unauthorized use and unauthorized alteration. It also undertakes to call on all third parties to whom the data is transmitted or transferred with the consent of the Customers to comply with the data security requirement.
The data controller shall ensure that the processed data cannot be accessed, disclosed, transmitted, modified or deleted by unauthorized persons. The Data Controlled may be accessed to the extent lawful only by the Data Controller and its authorized employees, the Data Controller's principals or the Data Processor used by it, and the Data Controller shall not transfer them to a third party who is not entitled to access the data.

The data controller will do everything in its power to ensure that the data is not accidentally damaged or destroyed. The Data Controller imposes the above commitment on the employees participating in the data management activities.

The following data protection solutions are available from the data controller:

- paper-based data carriers are placed in a lockable room
  access is restricted to those entitled to it;
- computer media are equipped with surge protection in the event of a power failure
  in the case of;
- computer media are protected by a firewall and antivirus;
- computer media are protected from internal intrusion by computer users
  your account is password protected;
- Data controller has a shredding device.

Data processing is secure for privacy impact assessment.

9.) DATA PROTECTION INCIDENTS MANAGEMENT AND REPORTING

A data protection incident is any event that involves the unlawful handling or processing of personal data in connection with personal data handled, transmitted, stored or processed by the Data Controller, in particular unauthorized or accidental access, alteration, communication, deletion, loss or destruction and accidental destruction and resulting in injury.

The Data Controller shall, without undue delay, but no later than 72 hours after becoming aware of the data protection incident, notify the NAIH of the data protection incident, unless the Data Controller can prove that the data protection incident is unlikely to occur.
risk to the rights and freedoms of natural persons. If the notification cannot be made within 72 hours, the reason for the delay shall be stated and the required information may be provided in detail without further undue delay.
Notification to NAIH
contains at least the following information:

- the nature of the data protection incident, the number and category of data subjects and personal data;
- Name and contact details of the data controller;
- the likely consequences of the data protection incident;
- the measures taken or planned to deal with the data protection incident,
  remedy.

The Data Controller shall inform the data subjects about the data protection incident via the Data Controller's website within 72 hours after the detection of the data protection incident. The information shall contain at least the information specified in this point.

The Data Controller keeps a record of data protection incidents in order to monitor the measures related to the data protection incident and to inform the data subjects. The register shall contain the following information:

- the scope of the personal data concerned;
- scope and number of stakeholders;
- the date of the data protection incident;
- the circumstances and effects of the data protection incident;
- measures taken to deal with the data protection incident.

The data contained in the register shall be kept by the Data Controller for 5 years from the detection of the data protection incident.

10.) ENFORCEMENT OPTIONS

The Data Controller makes every effort to process personal data in accordance with the applicable legislation, however, if the Customer feels that this has not been complied with, it is possible to write to the e-mail address additive@flono.hu or 3742 Rudolftelep, József Attila utca 5. posts
address.

If the Customer feels that his / her right to the protection of personal data has been violated, he / she may lodge a complaint with the **National Data Protection and Information Authority:** Name: National Data Protection and Information Authority
Headquarters: 105-11 Budapest, Falk Miksa utca 9-11.
Postal address: 1363 Budapest, Pf .: 9.
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
Website: http://naih.hu
Complaint handling: http://www.naih.hu/panaszuegyintezes-rendje.html

JUDICIAL ENFORCEMENT

The Data Controller is obliged to prove that the data processing complies with the provisions of the law.
The recipient of the data must prove the lawfulness of the data transfer. The trial will be heard by a court
falls within its competence. Thus, the action may, at the option of the person concerned, be brought before the court of the place where the person concerned is domiciled or resident.

A party who does not otherwise have legal capacity to sue may also be a party to a lawsuit. The Authority may intervene in the proceedings in order for the person concerned to succeed. If the court grants the request, it obliges the Data Controller to provide the information, to correct, block, delete the data, to annul the decision made by the automated data processing, to take into account the data subject's right to protest, or to release the data requested by the data recipient.

If the court rejects the data recipient's request, the Data Controller shall delete the personal data of the data subject within 3 days from the notification of the judgment. The Data Controller is obliged to delete the data even if the data recipient does not go to court within the specified time limit.
The court may order the execution of its judgment by publishing the identification data of the Data Controller.
disclosure is required in the interests of data protection and the protected rights of a larger number of data subjects.

INDEMNIFICATION AND DAMAGES

If the Data Controller violates the data subject's right to privacy by illegally processing the data subject's data or violating the data security requirements, the Data Controller may claim damages from the Data Controller. The Data Controller is liable to the data subject for the damage caused by the data processor and the Data Controller is also obliged to pay the data subject the indemnity fee for the personal data violation caused by the data processor. The Data Controller
shall be released from liability for damages and from the obligation to pay damages if
proves that the damage or violation of the data subject's right to privacy is outside the scope of data processing
rain caused an unavoidable cause.

No damages shall be payable and no damages shall be payable in so far as the damage was caused by the intentional or grossly negligent conduct of the injured party or the breach of the right to privacy.

The version number of this Privacy Policy is v1.0.
Present v1.0. The Data Management Policy No. is valid from April 25, 2022.