Privacy Policy

Privacy Policy

New Fire Technology Plc.

It is an important objective for the New Fire Technology Plc. (furthermore referred to as "Operator") that the personal information provided by visitors (furthermore: Users) to the https://www.newfiretechnology.com website (hereinafter referred to as the "website") is protected, and that the personal rights of the visitors should not violated.

The Operator reserves the right to change the Privacy Policy by reconciling the legal background and other internal regulations in the meantime.

The Rules govern the data management activities that are available through the website, personally, by telephone, by e-mail, by fax and / or by other means or through a forum on the website of the Operator.

The Operator also seeks to comply with the recommendations of the National Data Protection and Information Authority, in particular its recommendation of 29 October 2015 on the privacy requirements for prior information (https://www.naih.hu/files/tajekoztato-ajanlas-v- 2015-10-09.pdf).

By using the Website, any of its Services or any of its Applications, you, as a User, allow, that the processing of your personal data will happen according to the provisions of this Privacy Policy.

At the data collection the Operator may provide information about the data handling related to operation of the Website and any other the Operator's services that are not listed in this Policy.

I. The purpose of the data management:

1. The primary purpose of this Policy is to define and observe the fundamental principles and provisions governing the management of the data of natural persons that are in contact with the Operator in order to protect the private sphere of natural persons in accordance with applicable legal regulations and official resolutions.

2. The goal of these Rules is to ensure that the Operator is in full compliance with the provisions of the applicable legislation on data protection, in particular but not limited to

- the Act CXII of 2011 on the right to informational self-determination and freedom of information,
- the regulation (EU) No 2016/679 of the European Parliament and of the Council (GDPR),
- in accordance with the CVIII Act of 2001 on certain aspects of electronic commerce services and informational social services,
- the Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers
- the Act XLVIII. Of 2008 on the Fundamental Terms and Limitations of Economic Advertising Activity

3. The Operator therefore considers it of the utmost importance and is committed to providing the Act CXII. Of 2011, on the right to informational self-determination and freedom of information for the person whose data are affected through the website or other forums and respects the data subjects and their right of information self-determination. It contributes to the creation of safe internet access for affected persons, in full compliance with the relevant applicable regulations.

- The purpose of the data management of the User is to offer services of the Website and in particular: to identify the User, to distinguish the User from the others, to prevent unauthorized access to the personal data, to forward the User data in case of a quotation request, a booked service or an order to identify of User rights (accessible sub-services); for the administration through the customer service of the service; contacting the User; sending a system message related to the Service; to secure the space for the User’s content (e.g.: service evaluation), to develop the services and increase the standards of the Website, raise the User experience; to ease the service research, booking and the request for quotation.
- The agent can use the User’s personal data for commercials with direct business acquisition purpose based on an individual agreement (e.g.: New Fire Technology newsletter, newsletter, e-DM, etc.).
- If the booking, the order or the purchase happened on the Website with a credit card, the New Fire Technology will forward the data (username, first name, last name, country, phone number, e-mail address) to the bank, virtual payment terminal operator indicated by the payment method, as data manager. The purpose of the data forwarding is: the customer service assistance for the users, the confirmation of transactions and fraud observation for users protection.

Data management is lawful when, and only when, at least one of the following conditions is met:

- The affected person has previously and voluntarily contributed to the handling of his personal data for one or more specific purposes;
- If the processing is necessary to fulfil a legal obligation for the data manager;
- The processing is necessary to fulfil a contract, in which contract the affected person is one of the parties, or which contract prior to its conclusion is indispensable for taking any action for the request of the affected person;
- Data processing is necessary to protect the vital interests of a natural person (e.g.: affected person);
- It is necessary for the implementation of the task conferred on the data manager in the framework of exercising of its official powers or if managing the data is in the public interest.
- Data processing is necessary to enable the data manager or the legitimate interests of a third party to be covered by an exception if the interests or fundamental rights and freedoms of the data subject which necessitate the protection of personal data, in particular, the child concerned shall be given priority over the abovementioned provision of interest.
- The previous point does not apply to the handling of data carried out by public authorities in the performance of their duties.

To summarize:

The purpose of the data management:

- The identification of the beneficiary who ordered or purchased a services, requested a qutation through the website.
- In case of sending letters with commercial content, the purpose of the data management is to send commercial letters via e-mail to the customers.
- In case of sending newsletters or DM, the purpose of the data management is to forward them via e-mail to the possible customers.

II. The nature of the data manager and data processor

Data manager: New Fire Technology Public Limited Company, Seat: H-1165, Budapest Kalitka street 2., Registration number: 01-10-048978, Tax number: 25749953-2-42, Customer Service: info.newfiretechnology@gmail.com, https://www.newfiretechnology.com

A data manager assistant is the person whose activity has full responsibility by the Operator for the persons concerned and to third parties.
Service Providers act as an independent data managers for personal data made available for booking, quoting, and vouching.

With regard to direct marketing or marketing advertising (e.g.: Newsletter, e-DM), the Operator manages the User's data independently.

III. The validity of the code

1. Validity date: The current code is valid from 1 January 2024. until following regulations or the cancellation.

2. The personal scope expand to

- The data manager, furthermore
- The assistants, partners; as well as
- Those persons whose data are contained by the data management of this code, and
- Those persons whose rights or legitimate interests are affected by this data management.

3. Referring for those who were determined in the previous point, the affected persons are defined as the followings. The Operator handle the data for those natural and not legal persons, who

- connected the Operator in order to establish a customer relationship through phone or send their data via e-mail, on the Website or through Facebook or
- they did the same for another purpose such as applying a job by the Operator, or
- they use personally the services of the Operator.
- are in relationship with the Operator as Partners or Coworkers.

4. The material scope expands to every personal data in all organizational units of the Operator, whether if it is done electronically and / or on paper.

IV. Concepts

- The terms used in the Privacy Statement are contained in Act CXII of 2011 on Information Freedom and Information of Self-Determination law. (Info Törvény) http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.322945.
- It has to be interpreted according to the terms defined in the Interpretative provisions and the Terms of Use.
- According to the Info act:

Personal data: Data relating to the affected person, in particular the name, identification number, and the characteristics of one or more physical, physiological, mental, economic, cultural or social identities about the subject of the data, as well as the conclusion that may be deduced from the data;
affected person: any directly or indirectly determined natural person based on personal data.

contribution: a voluntary and explicit statement of the will of the affected person, which is based on an appropriate information network and which gives his / her unambiguous approval to the handling of his or her personal data, covering all or part of the operations.
data management: means any operation made irrespectively the method used on the data, such as collecting, recording, capturing, organizing, storing, modifying, using, querying, forwarding, publishing, aligning or linking, blocking, deleting, destroying data, and preventing future use of data as taking photograph or images, recording sounds and physical characteristics (e.g.: finger or palm print, DNA sample, iris image), which are suitable to identify the person.

data manager: A natural or legal person or a non-legal entity that independently or with others determines the purpose of the data processing, makes and executes decisions on data management (including the equipment used) or performs and executes it with a data processor entrusted.
data forwarding: Making the data available to a specific third party.

disclosure: Making the data available to anyone.
data deletion: making data unrecognizable in such a way that their recovery is no longer possible.
data marking: Providing an identification code to the data in order to differ from others.
data blocking: Providing an identification code to the data in order to limit temporary or permanently its further handling.

data processing: Performing technical tasks related to data management operations, regardless of the method and device used to perform the operations and to the location of the application, if the technical task is carried out on the data.
data processor: means a natural or legal person or an organization without legal personality who processes data on the basis of a contract concluded with the data manager, including the conclusion of a contract under the law.

V. The principles of the data management

- The Operator manages the recorded personal data according to the current data protection laws, in particular with the Regulation (EU) 2016/679 (GDPR) of the European Parliament and of the Council and with the Info Act, with international conventions on data protection, EU acts and other applicable laws, in accordance with the current regulations.
- The provisions of the current rules and the practice of the Operator may not stand against the data management principles.
- Personal data can be handled only for a specific purpose, to exercise the rights and fulfill the obligations. All stages of data management have to satisfy the purpose of data management, while the record and the management of data must be fair and legitimate. The principle of purpose must be enforced.
- Only those data can be handled which are necessary to the purpose of the data management, and it is suitable to reach these goals. Personal data can only be handled for the necessary duration and measure to achieve the goal. Accordingly, the Operator can handle only and exclusively those data that is strictly necessary. The principle of proportionality and necessity should be enforced.
- Personal data must be handled as a personal data while relationship with the affected person can be restored. The relationship can be restored if the Operator has the technical conditions that are required for recovery.
- Data management shall ensure the accuracy and completeness of the data and, if necessary for the purposes of data management, the updating of the data and the identification of the data subject for the time necessary for the purpose of data management.
- By using the appropriate security dispatch, the Operator cares about the accidental or unlawful destruction or accidental loss or unauthorized access, modification or spreading in order to save the personal data, stored in the automated data files.
- Data supply by the data subject is voluntary. The Operator treats personal data with the approval of the affected person. As a voluntary approval, as an agreement, you must understand the user behavior, which means that the user accepts that with the use of the website, all of the rules are automatically covered.
- The Operator forwards the personal data to a third party exceptionally and merges them only in that case if the person agrees in or the law permits and if the terms of the data management are met with each personal data. The Operator will forward the managed database to any other Operator, or business partners only if a reservation, an order or a quotation was made for a service provided by the Operator. The reservation means the explicit agreement of the affected person, since there is no such service what can be ordered without the transfer of data.
- In accordance with the services of the Operator and the purpose of data management, the person explicitly accepts that his / her personal data may be forwarded by the Operator to the Partner (s), if the Partner (s) was named and the activity of the Partner

(s) facilitate the fulfillment of the service issued to the beneficiary. The Operator excludes the liability on the unlawful data management of the Partners contracted with the Operator.

- The Operator does not forward any personal data to another Operator or Data Processor in a third country.

VI. The legal base of the data management

1. The record and the handling of the personal data in accordance with the operation and services of the website based on the affected person's individual approval and the data manager has provided prior information.

2. The preliminary consent must be admissible only if it fulfils all the three substantive requirements. The three requirements are:

- Volunteering,
- The definiteness (clarity)
- The awareness

3. The User gives his / her approval by using the services of the Website (e.g.: request, order, etc.).

4. The data manager manages the personal data with the consent of the affected person, in the event of its voluntary consent. In the voluntary consent, as an agreement, that consent is also included, when by using the website, the affected person accepts every regulation related to the use of the website, including the usage of this privacy policy, and by this it automatically expands to the affected person.

5. A clear consequence of the consent is that the data subject accepts the fact of the processing. If the processing is based on the voluntary consent of the affected person, in doubtful cases the data manager has an obligation to prove that he has given the relevant consent to the data handling processes.

6. The User may approve the use of his / her personal data for direct marketing or advertising purposes (eg Newsletter, e-DM), which may be withdrawn from the Operator at any time without limitation or justification. The User may also grant his / her consent by ticking a separate check box during the use of certain services (e.g.: ordering, booking, price quotation request).

7. If the affected person provides a written consent declaration that it applies to other transactions, these other matters shall be preceded by a clearly distinguishable method of application. It is important that it is easily understandable and readily available, clear and has simple language.

8. The affected person shall be entitled to withdraw his consent at any time, the data manager hereby informs the data subjects.

9. Withdrawal of consent does not affect the legality of the data handling prior to the revocation, which therefore does not have retroactive effect, is limited to the future processing of data.

10. If the affected person is unable to give his consent, because of his incapacity or for other unavoidable reasons, the Act CXII of 2011 states that, to the extent necessary, the personal data of the affected person may be dealt with in the existence of the obstacles to the consent, protection of the vital interests of itself or of other persons, and the life, physical integrity or property of the persons imminent threat thereof.

11. The statutory representative can give a contribution on behalf of a minor who is not older than 14 and instead of other incapacitated User. A User between the age 14 and 16 or who has limited incapacity can give his / her contribution with the approval or with a late consent of a statutory representative for the data management. A User over the age 16. can give an independent contribution. His / her legal declaration does not need the approval or the late consent of a statutory representative. The Operator cannot check the authority of the contributory person or the content about the statement of the legal representative, so the User or his / her legal representative have to guarantee that the contribution is in accordance with the law. The Operator considers the appropriate consent of the legitimate representative to be given.

12. The User warrants that the affected person acquired legally the contribution to make a third natural person available to the data management through a service.

13. In the absence of a different provision of the law, the Operator can publish the personal data in order to fulfill its legal obligations (in particular the accounting liabilities, or the obligation to the contractual Partners) or to enforce the legitimate interests of its own or a third party without any contribution, if these enforcements meet with the proportion of the limitation about the personal data security law. The Operator can do it even if the User has withdrawn its contribution.

VII. Scope of the managed data

- The User has the responsibility for the authenticity and accuracy of the personal data.

The range of the handled personal data is influenced by the nature of the Services, the e-commerce, accounting and advertising rules, and in particular the Act of CVIII of 2001 13/A on certain aspects of electronic commerce services and information society services and the Act XLVIII of 2008 Section 6 on the Fundamental Terms and Limitations of Economic Advertising Activity.

- **Quotation request, Order, Social Media**

In these cases, the range of affected persons: Any natural person who intends to contact the data manager, to call for proposals, order, or receive news, promotions and discounts regularly, therefore, by entering your personal data you subscribe to the DM and newsletter service of the Data Manager.

Data managed in case of reservation and request of quotation might consist of: Name, email address, phone number, address (country, postal code, settlement, street name and house number), possible tax number. During reservation and request for quotation the User is able to share further personal data in the comment section with the Partner intermediating the offer and the Intermediary.

Request for quotation

The activity and process involved in data management are as follows:

1. The affected person may consult with the Data Manager by completing the text boxes on the interface located in the "Contact" section of the website and by clicking on the "Send" button or by other means or by using another forum to consult with the Data Manager of its services and/or other related issues.
2. The information provided to the data manager through the website shall be sent via e-mail.
3. The staff member shall answer the question of the matter concerned and shall circulate it, on the same path as the information received, if it does not otherwise provide.

Scope of managed data:

- Name
- E-mail Address

Duration of data management: it lasts until the target is fulfilled.

Order

The activity and process involved in data management are as follows:

1. Submit information and order request to the data manager, as available or through the forum.
2. The data manager shall contact the contact data provided by the affected person and agree on the request for the order and provide free information about the data manager's services.
3. During the contact, other data in possession of the Data Manager, such as the operational and other data pertaining to the company concerned, the Data Manager shall link the data provided by the information subject and treat it as business secret.
4. The data manager shall either give the affected person a request or submit a contract of service after clarification of the order requirements.
5. After signing the contract, the Data Manager shall commence the affected person to the performance of the services.
6. After completion of the contract, the data manager and the affected person shall record a performance certificate or minutes (report).
7. The data manager stores the contracts and the performance certificates in accordance with its own archiving rules.
8. The affected person will voluntarily contribute to providing an e-mail address and/or telephone number when submitting an order request, so that the data manager can contact him/her to make the order more precise or that the affected person can confirm its order.

The data manager communicates only with the affected persons and therefore the purpose of the information becomes relevant when the affected person locates the data manager through the community site.

Scope of managed data:

- Name
- E-mail Address

Duration of data management: it lasts until the target is fulfilled.

Social Media

1. The purpose of presence and data management on community portals, particularly Facebook, is to share, publish and marketing content on the website on the community side. You can also use the community site to find out about the latest promotions.
2. The affected person will voluntarily contribute to the tracking of the contents of the data manager, based on the conditions of the community site. As an example, the affected person can subscribe to the news feeds published on the Facebook messaging wall, by clicking on the "like"/"tetszik" link on the page and contributing to the publication of news and offers from the data manager. You can sign up on your wall and click the "Dislike"/"Nem tetszik" link in the same location and you can use the message wall settings to clear news feeds from unwanted message walls.
3. The data manager in question can be evaluated in text and numerically if this community site allows it.
4. The data manager's community page, in particular the Facebook page, will also publish images/video footage of various events, data management services and more. The Data Manager may link the Facebook page with other community sites according to the rules of the Facebook.com Community portal, so publishing on Facebook will have to be understood as publishing on these related social portals.
5. If the case is not mass recording or the inclusion of a public image (PTK. 2:48 §), a data manager shall always consult the written consent of the affected person before publishing the images.
6. Information on data management for the relevant community site can be found on the relevant community page, for information on Facebook page data management, see facebook.com.

Scope of managed data:

- Name
- E-mail Address

Duration of data management: it lasts until the target is fulfilled.

- **Evaluation**

In case of a successful reservation, the Intermediary has the possibility to ask for an evaluation from the User who resorted the service. The reviews and ratings of the service made available by the user – with settlement given by address, and with or without name depending on the decision of the user – can be made publicly available for everyone.

- **Marketing requests**

Data managed by New Fire Technology Plc. in case of a request for direct acquisition of business with advertising content and a request with marketing purpose respectively consist of: First and Last name, email address, and behavior of the user (e.g.: orders, reservations, requests for quotation etc.)

The affected person can subscribe to the newsletter before or during the use of the services or by any other means, such as through the website.: Name, E-mail Address

Subscription to the newsletter is based on a voluntary contribution.

Scope of managed data:

- Name
- E-mail Address

The purpose of the newsletter submission is to provide the recipient with complete general or personalised information about the latest actions, events, news, Notification Services, and non-availability of the data manager.

A newsletter is sent only with the prior consent of the relevant person.

The Data Manager reviews the newsletter list every three years and asks for a confirmatory contribution for the submission of the newsletter after three. The data of the affected person which does not provide a confirmatory contribution for the sending of the newsletter within 15 days of the date of receipt of the confirmatory letter will be erased from the data file by the data manager on the following day (16th day).

The Data Manager will report statistics on the reading of newsletters, through clicks on links in newsletters.

To subscribe to the news stream published on the social networks, especially on the Facebook page, you can sign up by clicking on the "like"/"tetszik" link on the site and by clicking on the "Dislike"/"Do not like" link in the same location Or you can use the message wall settings to clear news feeds that appear on unwanted message walls. For information on social networking, news feeds, subscriptions, and communications from a community site, see the Community page.

Duration of data management: until the deletion of the affected person.

- **Prize Competition (Prize Game)**

Participation in the lottery is based on voluntary contributions.

Scope of the data subjects: any natural person who wishes to participate in the prize game organized by the data manager.

Scope and purpose of managed data:

- First Name – identification, basis of the draw
- Phone Number – Contacts
- E-mail Address – Contacts

The purpose of data management is to identify those affected by the draw (lottery), as well as to maintain contacts.

The activity and process involved in data management are as follows:

1. According to the rules of the sweepstakes, you are concerned to enter the prize game by entering your details.
2. The data manager shall record the data electronically and/or on a paper basis according to the rules of the game and carry out the draw.
3. The Data Manager shall notify the winners on their specific contact details.
4. The Data Manager may make the names of the winners available to other stakeholders, as well as third parties, according to the rules of the game, and therefore calls attention to the data subjects to consider the participation.
5. In accordance with the purpose of the processing, the affected person will voluntarily contribute to the contact of the Data Manager, through his specific contact details, to inform him of the possible inability to give the lottery, or to clarify the receipt of the prize, answer any complaint or take any other action relating to its complaint.

Duration of data management: Until target has been achieved.

An individual data file is generated for each data management and therefore all data management is required to be reported.

VIII. Data transmission

- **Reservation, Request for quotation**

In case of reservation and request for quotation the Operator - based on the voluntary approval of the user – forwards the User's personal data (name, e-mail address, phone number, number and age of children, data over pet keeping), remarks and preferred paying method with the reservation, request for quotation to the Partner intermediating the offer, with a purpose for quotation.

IX. Duration of data management

- **Data managed due to recourse of services**

The Operator manages personal data connected to an order or a request for quotation, initiated and accepted by the User, as reservation data. In case of a declined quotation personal data is managed for 6 months. The Operator keeps personal data to fulfill its obligation towards accounting and Partners according to Section 169 of Act C of 2000, for 8 years, and for the term of limitation specified by the Act XCII of 2003 on order of taxation.

- **Data managed due to requests**

The Operator manages the personal data of the User until the cancellation by the User for direct acquisition of business with advertising content and requests with marketing purpose. The termination of some services on the Web page and the removal of the Facebook application does not result in the cancellation of the approval for direct acquisition of business with advertising content and requests with marketing purpose. The approval must be cancelled separately according to request type (e.g.: New Fire Technology newsletter, e-DM, etc.).

- **Customer Service**

The Operator stores the complaints, questions and requests sent to the customer service for 6 months after the date of submission, and then deletes them – with the exception of correspondence in pending cases.

X. Modification, removal and distraint of data, recrimination against data management

1. The User may primarily ask the Operator for modification of data, given during the process of reservation and request for quotation, through the contact channels given by the Operator. If the User asks the Operator for modification of data through the e-mail address of the customer service, The Operator will forward the Users request to the Partner.
2. The approval, given for direct acquisition of business with advertising content and requests with marketing purpose, can be withdrawn separately, depending on request type (e.g.: New Fire Technology newsletter, e-DM), by the link at the bottom of the electronic mail, or through the info.newfiretechnology@gmail.com e-mail address, or at the postal address of New Fire Technology Plc..
3. Distinctly from the above mentioned cases – except for the so-called mandatory data management – the User may send an e-mail to the info.newfiretechnology@gmail.com e-mail address to ask for the removal of personal data from the Operator. The Operator removes the User's personal data even without the request of the User, if the management of the above mentioned data is illicit, the purpose of managing data ceases; or the statutory deadline for storage of data expires; it is ordered by the court or by the National Authority for Data Protection and Freedom of Information; or if the data management is incomplete or incorrect – and this condition can not be legally remedied -, provided that the removal of data is not excluded by the law. The Operator locks personal data instead of deleting it, if the User asks for it, or based on the information available, it may be assumed that the deletion of personal data would undermine the legitimate interests of the User. The locked personal data will only be handled by the Operator as long as there is a purpose for data management that excludes the deletion of the personal data. After the withdrawal of the User's consent, the Operator may henceforward manage the personal data of the person concerned according to section IX.
4. The User may exclaim against the management of his/her personal data by sending an e-mail to info.newfiretechnology@gmail.com, the customer service e-mail address,
    1. if the management or handling of data is necessary solely for the fulfillment of the legal obligations of the Operator, or for the validity of the legitimate interests of the Operator, data recipient or third party, except for the so-called compulsory data management;
    2. if the use or transfer of personal data is done for the purpose of direct acquisition, survey or scientific research, as well as
    3. in any other case specified by the law.
5. If the Operator determines the validity of the User's objection, data management – including further data collection and possible transfer of data – will be terminated and the data will be blocked. Furthermore the Operator will inform those who have been transferred data about the User who is subject to the objection, and who are obliged to take action to fulfill the right of objection.
6. If the data management (e.g.: accounting) has been prescribed by the law, the Operator cannot delete the User's data but will not transfer the personal data to the data receiver if it has agreed with the protest or the court found the protest lawful.

XI. Requesting information

- The User may at any time request information about the personal data handled by the Operator in connection with the services of the Website at the info.newfiretechnology@gmail.com email address. At the request of the User, the Operator provides information on the User's data processed by or managed by the data processor in connection with the given service, their source, the purpose, legal basis, duration of the data processing, the name and address of the data processor, legal basis and addressee

of the data transfer, its data management related activities. The Operator shall provide the requested information within 30 days of the submission of the application.

- The Act CXII of 2011 and article 15 of Regulation (EC) No 2016/679. The affected person has an information right, or "right of access". During the enforcement of the law, the Data Manager provides information about:

1. The data it manages
2. Categories of personal Data
3. The purpose of the data management,
4. The legal basis for the processing of data,
5. duration of the processing,
6. Where appropriate, the period of storage of data or, if this is not possible, the criteria for determining that period,
7. Where appropriate, if the information has not been collected from the affected person, any available information on their source,
8. Where applicable, automated decision-making, including profiling, and logic and understandable information about the significance of such processing and the likely consequences for the affected person,
9. Information on the data processing in the case if a processor has been used,
10. The circumstances, effects and measures taken to avert the data protection incident, and the
11. In the case of transmission of personal data to the affected person, the legal basis, purpose and addressee of the transmission.

?

- This information shall be free of charge if an information request for the Data Manager for the same data range has not yet been submitted by the person requesting the information in the calendar year. In other cases, costs may be imposed on the requesting information. If the data have been unlawfully handled or the request for information has resulted in an adjustment, the reimbursement of expenses already paid shall be refunded.
- By the power of the court, public prosecutor's office, detective authority, offense authority, administrative authority, National Authority for Data Protection and Freedom of Information or a statute, other bodies may request the Operator to provide information, transmit data, or provide documentation. The Operator will provide the requesting body with the personal data that is indispensable for the purpose of the request, provided the exact purpose and scope of the data is indicated.
- Based on the Act CXII of 2011, information should be refused. The Data Manager hereby invites the attention of the data subjects. On the basis of the law, information must be withheld:
  - If, on the basis of a statute or an international treaty or a statutory act of the European Union, the data manager takes personal data as an affected person, that the transmission data manager will, at the time of the transfer, indicate the affected person of the personal data Rights under the law or other restrictions of its treatment.
  - in order to the external and internal security of the state, such as Defence, National security, prevention or prosecution of criminal offences, In order to ensure the sentence-execution, also State or municipal economic or financial interests, The significant economic or financial interests of the European Union, Disciplinary and ethical offences relating to the exercise of occupations, To prevent and detect labour and safety breaches, including in all cases monitoring and surveillance, - including monitoring and surveillance in all cases -, also to protect the rights of the affected person or of others.
- The Data Manager shall notify the National Data Protection and Information Freedom Authority annually by 31 January of the year following the year in which the information applications are refused.

XII. Request for correction, deletion, restriction, blocking

- The right of correction: the affected person may legitimately initiate the correction of inaccurate personal data which the data manager is required to implement without undue delay. Depending on the objective of the processing, the affected person is entitled to request the completion of incomplete personal data, by means of an additional declaration. However, the data manager is required to adjust, even without the request of the affected person, the personal information, if the personal information is not true and the true personal data is available to the data manager.
- in Act CXII of 2011 and under Regulation (EC) No 2016/679 of the European Parliament and of the Council the Data Manager is obliged to delete the data (other than in the above case) if the treatment of the data is unlawful;

1. The data is incomplete or incorrect-and this condition cannot be legally remedied-provided that such deletion is not ruled out by a law;
2. The purpose of the data management has ceased or the date of storage of data by the law has expired;
3. It has been ordered by the court or the authority.
4. Personal data are no longer required for the purposes for which they were collected or otherwise treated;
5. The affected person is in protest against data processing, and there are no priority lawful reasons for processing information;
6. Personal data shall be deleted to fulfil the legal obligation imposed by the law applicable to the data manager;
7. Personal data collection, as mentioned in Paragraph 1 of Article 8 in the EU Act 679 of 2016, was conducted in connection with the provision of information society services directly to children.

- If the data manager has made public a personal information for one reason and is obliged to delete the foregoing, it shall take reasonable steps to inform the other data managers handling the data that the data subject initiated the links to the personal data in question or the deletion of a copy or duplicate of this personal data. This should be done taking into account available technology and the costs of implementation, including technical measures.
- The data manager informs the affected person of the limits of the deletion or of the "Right to be forgotten" EU regulation:

1. Exercising the right to freedom of expression and orientation;
2. Execution of an obligation on the processing of personal data, in accordance with EU or Member State law applicable to the manager, and the execution of a task in the public interest or in the exercise of a driving licence conferred on the affected person;
3. Public interest in the sphere of health;
4. In accordance with Paragraph 1 of Article 89 of Regulation (EC) No 2016/679, for archival purposes of general interest, for scientific and historical research purposes or for statistical purposes, if the right to delete would be likely to render impossible or seriously could jeopardize this data management; Or
5. Proposing, validating or defending legal claims.

- The right to restrict the processing of data or to blocking them: The affected person may initiate a restriction on the processing by the data manager.
- If the deletion would violate the legitimate interests of the affected person, the information should be blocked, only if it can be assumed on the basis of the information available to him. The personal data locked in this way can only be handled as long as the privacy policy in place is in effect, excluding the deletion of personal data. The data shall be clearly blocked if the affected person disputes the accuracy and correctness of the personal data and the incorrectness or inaccurateness of the data (s) in question cannot be determined. In this case, the locking period shall be valid until the data manager verifies the accuracy of the personal data.
- The data should be blocked under the EU regulation if

1. The processing is unlawful and the affected person opposes its deletion and, instead, asks for restrictions on its use;
2. The data manager no longer needs personal data for the purpose of data management, but the affected person does not require them to submit, validate or protect legal claims; Or
3. The affected person objected to the processing of data; In this case, the restriction shall apply for a period of time until it is established that the legitimate grounds of the data manager take precedence over the legitimate reasons for the affected person.

- Locked data (other than storage) can only be treated if the affected person agrees or is necessary for the submission, validation or protection of legal claims, or for the rights of other natural or legal persons Interests of the Union or of a Member State.
- The law may restrict the right of the relevant rectification, erasing or freezing to the internal and external security of the state. This includes the following:

1. Defence
2. The National security
3. The prevention or prosecution of criminal offences
4. The sentence-execution
5. State or municipal economic or financial interests.
6. The significant economic or financial interests of the European Union,
7. Disciplinary and ethical offences relating to the exercise of occupations,
8. To prevent and detect labour and safety breaches, including in all cases monitoring and surveillance,
9. To protect the rights of the affected person or of others.

- The data manager is obliged to inform the affected person of his decision on the application within 15 days of receipt of the request, if it does not justify his delay and/or corrects and/or cancels and/or locks the data or take any other steps according to the request if there are no grounds for refusal.
- The data manager shall inform in writing the particulars concerned of any rectiation, erasures or limitations on the processing of data, as well as any persons who previously transmitted the data (s) for the purposes of the data handling. If requested by the affected person, the data manager shall inform them of such recipients. Where it does not prejudice the legitimate interest of the affected person in view of the handling of the information or if the provision of information proves impossible or involves a disproportionate effort, the notification may be dispensed with. The data manager shall also be obliged to notify the affected person in writing if, for any reason, the right of the affected person cannot be met and must indicate precisely the factual and legal cause and the remedies open to the affected person: the possibility of contacting the National Data Protection and Information Authority and the Court.

XIII. Validation of claims

- A request from the email address previously given to the Operator is considered by the Operator as a request from the User. In case of any other email address or in writing, the User may submit a claim if – as determined by the Operator or by law – he/she has properly verified the User's identity.
- If the data management of the Operator is not based on the consent of the person concerned, but the data processing has been initiated abusively by a third party, the person concerned may request the deletion of any personal data disclosed by the User and any information related to the management of data, in accordance with verifying his/her identity and relationship with the personal data.
- In the event of the death of the User, by submitting the death certificate or sending a copy of the death certificate to newfiretechnology@gmail.com customer support, any close relative of the User or the person who has been beneficiary of the testament may request the deletion of the User's Data, besides confirming the relationship with the User.

XIV. Law enforcement options

- The right to protest: the treatment of your personal data and your profiling may protest the

1. The processing of personal data (transmission) is necessary only to enforce the right or legitimate interest of the data manager or the data importer, except in the case of compulsory data processing;
2. The use or transmission of personal data is done for direct marketing, public opinion research or scientific research;
3. The exercise of the right of protest is otherwise permitted by law

- The data manager shall examine the objection and shall inform the applicant in writing of the outcome as soon as possible after submission of the application, but not later than 15 days. This involves the simultaneous suspension of data handling. If the applicant's objection is well founded, the data Manager shall terminate the handling of the information, the further recording and transmission of data. It shall also block the data and notify the fact of the objection and of the measures and decisions taken thereunder, all the partners to whom the personal data of the affected person by the protest has previously been transmitted. In addition, the notified persons are obliged to take action to enforce the right of protest.
- If the affected person does not agree with the decision of the data manager or if the data manager fails to abide by the referenced time-limit, the affected person is entitled to apply to the court within 30 days of notification of the decision.
- Law enforcement (jogérvényesítés): The affected person may apply to the court for violation of his rights. The court treats the case as an expeditious procedure (gyorsított eljárás). The data manager must demonstrate that the data handling is the same as in the current legislation. http://www.1moment.hu/szotar.pdf
- Statutory rules on compensation and tort (sérelemdíj-tort, penalty): If the data manager infringes the personal right of the affected person by breaches of the unlawful handling of the data concerned or of the requirements of the security, the affected person shall have the right to claim a violation of the data manager.
- In case of alleged infringement of the personal data of person concerned, he/she may contact the competent court, the Budapest Metropolitan Court in the capital or initiate an investigation with the National Authority for Data Protection and Freedom of Information (president: dr. Attila Péterfalvi, 1024 Budapest, Szilágyi Erzsébet fasor 22/C., ugyfelszolgalat@naih.hu, +36-1-3911400, www.naih.hu).

XV. Data security

- The Operator will take the necessary technical and organizational measures, and establish the necessary procedural rules in order to ensure the security of the personal data provided or made available by the User during the entire process of data management.· The Operator stores the personal information of the Users in Hungary, Budapest, 1165. Kalitka street 2. at their guarded headquarters equipped with alarms.· The Operator, as a data manager, guarantees, in particular as regards competence, reliability and resources, that it implements technical and organisational measures to ensure that its requirements are met, including security of data management Regulation (EC) No 2016/679 of the European Parliament and of the Council (GDPR) and the Info law - in accordance with the international conventions on data protection· The Operator shall ensure that persons authorized to have access to the personal data of the affected person - if they are not otherwise subject to an

appropriate legal secrecy obligation - are bound by secrecy with regard to the personal data they have known.

- The Operator has appropriate hardware and software tools, and undertakes to implement technical and organisational measures to ensure the legality of the processing and rights of the data subjects.· The IT protection tasks require priority care from the data manager, in particular:
- Measures to ensure protection against unauthorised access, including protection of software and hardware devices and physical protection (Access Protection, network protection);
- Measures to ensure the possibility of restoring data files, including regular backups and separate and secure management of copies (mirroring, Backup);
- Protection of files against viruses (virus protection).
- Physical protection of files and/or of the devices bearing them, including fire damage, water damage, lightning strike, other elemental damage protection, and the recovery of any damage caused by such incidents (archiving, fire protection).

XVI. Log data

- During the use of the Website, data of the site visit and specific conversion events (e.g.: registration, reservation, request for quotation) will be recorded. The logging of these data is continuously carried out by the system to prevent abuses, produce statistics, monitor the functionality and performance of the services of the Website, and keeps personal information about the particular event.

XVII. Cookie

- For customized service and convenience features, the browser cookie stores for the last 6 services viewed, the date of the last check-in to the page, browser language, currency used, and newsletter popup closure for 30 days. The application of the browser cookie may be rejected by selecting the appropriate settings in the browser(s), but in this case the User will not be able to use this convenience feature.
- The Operator's website was created with the help of www.unas.hu portal, as the website uses this engine. Sites created through www.unas.hu and the portal may use the following cookies, but the Operator does not use these cookies in any way. The used cookies communicate between the User's device and the www.unas.hu portal, no data is transmitted or transferred to the Operator, so for the cookies used, www.unas.hu's own privacy policy is authoritative. The cookies that can be used by the www.unas.hu portal and the pages created with its help, and the purpose of these cookies:

1. Absolutely necessary cookies
    1. Such cookies are indispensable for the proper functioning of the website.
       Without the acceptance of these cookies, the Operator can not guarantee the proper functioning of the website or the user's access to any user-requested information.
    2. These cookies do not collect personal data from the person concerned, or any data that can be used for marketing purposes from.
    3. Cookies that are absolutely necessary are, for example, Power cookies that collect information about whether the website is working properly and whether it is experiencing any malfunctions. By indicating any defects, they help the Operator improve the website and indicate the most popular parts of the website.
2. Functional cookies
    1. These cookies ensure the website's consistent appearance for the needs of the person concerned, and memorize the settings chosen by the person concerned (such as color, font size, layout).
3. Targeted cookies
    1. Targeted cookies ensure that advertisments appearing on the website are aligned with the interests of the person concerned. The website primarily focuses on advertisements related to products and services provided by the Operator, and facilitates access to better offers for the person concerned
4. Cookies provided by a third party
    1. The website may display a cookie provided by a third party – such as a social networking site – that allows the user to share or like a content, and sends information to a third party, which they may use later to show advertisements to the person concerned on other websites as well.
5. Furthermore the cookie also helps to improve the website's ergonomics design, to create a user-friendly website to enhance the visitors' online experience.

XVIII. External intermediary service providers

- Providers of external services (such as Instagram, Twitter, Facebook) that make content sharing available on the various social networking sites are considered personal data controllers, and their activities are governed by their own terms of use and privacy policy. Also, the Operator of the given service acts as a data controller for the services that are embedded within the framework of the Services but are reserved by an external Operator (e.g.: "Ask us, we are responsible" provided by Facebook).
- When installing the applications available on the Operator's website, the Operator will be provided with personal information specified in the information made available by Facebook Inc. on the User's voluntary consent, subject to compliance with the Facebook Inc. Privacy Policy. If a Facebook application refers to this prospectus, the Data Handling Guide is relevant to the data management of the Operator. In addition, data management with Facebook services (e.g.: deletion of applications, posts, etc.) is governed by Facebook Privacy Policy. The Deletion of applications from Facebook user settings (https://www.facebook.com/settings?tab=applications) can be initiated (in the application menu).
- The Operator's website may also include links to sites that are not operated by the Operator, and only serve to inform visitors. The Operator has no influence on the content and security of the websites operated by partner companies, so it does not take responsibility for them.
- With respect to Section 155, paragraph 4, of Act C of 2003, the Operator considers that "Information may be stored in an electronic communications terminal equipment and the information stored there may be accessed using an electronic communications network exclusively on the basis of the consent of the user or subscriber following his clear and full information". The sections described in Section XVI. provide information about the analytical tools it uses, i.e. cookies.

XIX. Web analytical and ad-serving external companies

- For the functioning of the website the Operator uses external web analytics and ad-serving companies that perform their activities independently of the Operator.
- The Operator can use Google Inc.'s Google Analytics and Google Ads services. Google Inc. uses cookies and web beacon (web marker) for information gathering and in order to help analyse the use of the website. The information stored by the cookie (including the User's IP address) is stored by Google Inc. on its US servers. Google Inc. may transfer the information collected to third parties if this is required by law or processed by third parties on behalf of Google Inc. In case of Google Ads remarketing,

Google Inc. places tracking cookies on the User's device, which monitor the online behaviour of visitors, and on the basis of which Google Inc. makes advertisements based on user behaviour and interests available for them on other websites. The tracking cookie allows Google Inc. to identify the User on other websites as well. Google Inc.'s "Privacy Policy" is available at the http://www.google.hu/intl/hu/policies/privacy/ website. For more information on Google Inc.'s activity concerning data, how to disable cookies and personalize your ads visit the following website: http://www.google.hu/intl/hu/policies/privacy/key-terms/.

XX. Statement

The Operator declares that:

1. during the course of data management, the Operator considers Act CXII of 2011 law on rights of information self-determination, and freedom of information and the Regulation (EU) 2016/679 (GDPR) of the European Parliament and of the Council as compulsory.
2. personal data collected by the Operator during the course of data management can only be accessed by the Employees and external Partners who are responsible for the given data management.
3. in accordance with the principle of transparency, keeps the operative data protection rules at all times accessible to the person concerned, thereby enforcing the website's privacy, keeping the personal information of the visitor in accordance with the applicable legal regulations, ensuring the security, technical and organizational measures of those personal data, and sets up procedural rules to ensure that the principles of data protection are fully respected.
4. it will take all measures to facilitate information technology and other secure data management related to data storage, processing and data transfer in order to preserve the data it manages.
5. it will do its utmost to ensure the protection of personal data it manages against unauthorized access, alteration, disclosure, deletion, damage, and destruction to guarantee the necessary technical conditions.
6. it does not verify the personal information provided to it, and it will not take responsibility for the pertinence of them.
7. it only interconnects the database with another Operator, business Partners or transfers the personal data to a third party in exceptional cases and in the case in which the person concerned expressly agrees or it is permitted by the law, and if the conditions for data management are met for each personal data, or it is strictly necessary due to the performance of the service.
8. it does not belong to a multinational enterprise, therefore it does not need to introduce and operate mandatory organizational regulations.
9. it does not transmit or transfer personal information to a data processor in a third country.
10. it keeps a record of the transfer of datum or data to a domestic data controller containing the date of transmission of the personal data handled by the Operator, the legal basis and the addressee of the data transfer, the determination of the scope of the personal data transmitted and other data specified in the law for data processing.
11. it keeps a record in order to monitor data protection incidents and provide information to the person concerned, including the personal data concerned, the scope and number of persons involved in the data protection incident, the date, circumstances and effects of the data protection incident, and the measures taken to provide against the data protection incident,
    as well as any other data specified in the law that prescribes data management.
12. by using appropriate security measures to protect the personal data stored in automated data files, the Operator will ensure the prevention of accidental or unlawful destruction, and accidental loss or unauthorized access, alteration or dissemination of personal data.

XXI. Notification, making a complaint

1. Data manager shall ensure that the data subject declares his complaint concerning the service and/or the data manager's conduct, activity or omission orally (in person, by telephone) or in writing (delivered in person or by someone else through the document, by post, by electronic mail).

2. Range of data subjects means any natural person who wishes to present orally or in writing a complaint concerning the service provided and/or the data manager's conduct, activity or omission.

3. The treatment of managed data is to identify the complaint and to include obligations derived from the law. Range of data to be handled when filing a complaint:

- ID of the Complaint
- Name*
- Date of receipt of the complaint *
- Phone number
- Date of the call *
- Personal information provided during the conversation
- Billing/Mailing Address
- The complained service
- Attached documents
- Reason for the complaint *
- The complaint itself *

4. The purpose of data processing is to enable the notification of the complaint and to make contacts.

5. The activity and process involved in the data management are as follows:

1. The complaint is notified to the data manager orally (in person, by telephone) or in writing (by means of a document transmitted in person or by another, by post, by electronic mail)
2. Where the complaint is made orally, it shall add a record of the data manager's complaint form or the contents thereof.
3. If the affected person wishes to make his complaint in writing, he/she shall be able to do so.
4. The Data Manager shall process the complaint and answer as soon as possible.
5. The Data Manager shall endeavour to resolve any complaints as soon as possible, by common interests.

6. Duration of data processing: The data manager shall handle the report on the complaint and the copy of the reply for five years from the date of the recording with the relevant and in force pursuant to paragraph 7 of 17/A § of the Act CLV of 1997, the Act is compulsorily.

In case of violation of your rights to information autonomy, you may make a complaint or notification to:

National Authority for Data Protection and Freedom of Information

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Telephone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

In case of violation of minors, hate speech, exclusionary content, correction, rights of a deceased person, breach of good reputation

to, you may make a complaint to:

National Media and Intercommunications Authority
Address: 1015 Budapest, Ostrom street 23-25.
Mail address: 1525. Pf. 75
Telephone: (+36 1) 457 7100
Fax: (+36 1) 356 552
Budapest, 01.01.2024.

The present contract has been made in two languages (Hungarian, English). In case of any legal disputes, the Hungarian version of the contract must be considered the determinative one.

For questions not treated in the present contract, the facts stated in the Hungarian Civil Code has the authority.