Privacy Policy

Introduction

The Coolfire Limited Company (registered office: 1149 Budapest, Kövér Lajos u. 31-37., company registration number: Cg.01-09-912574 as a data controller (hereafter referred to as Data Manager), during the operation of www.coolfire.hu ("Prospectus") for your personal information. Commits to the all data management related to this activity is in accordance with this Code and the applicable national law legislation and the legal acts of the European Union.

Data Privacy Guidelines for Data Management Data Management are available at www.coolfire.hu. The Data Controller reserves the right to change this Information at any time, of course, informing its audience of any changes made in due time. If you have any questions about our present announcement, please write to us and our colleagues will answer your questions.

The Data Controller is committed to protecting the privacy of its customers and partners, and it is of paramount importance to respecting the privacy of their clients' information self-determination. The Data Handler manages the personal data in confidence and takes all security, technical and organizational measures that guarantee the security of the data.

As a Data Controller, the Data Administrator respects the privacy of all individuals for whom personal data is transferred and is committed to protecting them. Under Article 13 of the European Union General Data Protection Regulation (Decree 679/2016, 'the GDPR'), it provides the following information:

I.

Data manager

Data Controller Name: Coolfire Limited Liability Company
Headquarters: 1149 Budapest, Kövér lajos u. 31-37.,
Company registration number: Cg.01-09-912574
Registry authority: Fővárosi Törvényszék Cégbírósága
Tax number: 14628214-2-42.
Phone number:
For privacy inquiries, contact us at the following e-mail address:
info@coolfire.hu

II.

General Provisions

2.1. The personal and material scope of the information
The material scope of the prospectus covers www. coolfire.com is concerned with data management natural persons (hereinafter referred to as 'the data subject' or 'the data subject').

2.2 Concepts
"Data management" means personal data or data files in an automated or non-automated manner carried out any operation or operations, such as collecting, recording, organizing, dividing, storing, conversion or alteration, querying, inspecting, utilizing, transmitting, distributing or otherwise by way of disclosure, alignment or interconnection, restriction, deletion, or destruction;
"Processor" means any natural or legal person, public authority, agency or any other body, which handles personal data on behalf of the controller;

"Third party" means any natural or legal person, public authority, agency or any other body, which is not the same as the data subject, the data controller, the data processor, or the persons who are under the direct control of data controller or data processor, have been authorized to handle personal data;
"Personal data" means any information relating to an identified or identifiable natural person ("concerned"); the natural person who can identify, directly or indirectly, in particular an identifier such as name, number, positioning data, online identifier or natural person, physiological, genetic, spiritual, economic, cultural or social identity of one or more factors;
"IP Address": An IP address is a series of numbers that can uniquely identify the computers and mobile devices of affected Internet users. IP addresses can also geographically locate a visitor using that computer. The address of the pages visited, as well as the date and time data are not suitable for the identification of the subject, but are linked to other data (such as those provided during registration), which can be used to draw conclusions on the person concerned.

2.3. Principles
The Data Controller is responsible for:

- treats personal data legally and fairly and treats it transparently ("lawfulness, fairness and transparency");
- collects personal data for a specific, unambiguous and legitimate purpose and not treat them in a way that is incompatible with these goals ("purpose limitation");
- the manageable personal data are appropriate and relevant to the purposes of data management and are limited to the need ("saving of the data");
- ensures that personal data is accurate and, if necessary, up-to-date and takes all reasonable steps to delete or correct inaccurate personal data for the purposes of data management ("accuracy");
- keeps personal data in a form that allows the identification of the data subjects only for the time needed to manage the personal data ("limited storage");
- personal data is handled in such a way as to ensure adequate security of personal data, including the protection against unauthorized, unlawful, unintentional, loss, destruction or damage of data ("integrity and confidentiality") by means of appropriate technical or organizational measures.

2.4. Related Legislation

- 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 Directive 95/46 / Data Protection Regulation);
- 2011 CXII. law on information self-determination and freedom of information (Infotv.);
- CVIII. Act on Electronic Commerce Services and Certain Issues of Information Society Services (Eker law);
- Act C of 2003 on Electronic Communications (Eht.);
- XLVIII of 2008. Act on the Fundamental Terms and Limitations of Economic Advertising (Grt.);
- Act V of 2013 - Civil Code (Civil Code);
- 1997 CLV. Act on Consumer Protection.

III.
THE PURPOSE, PERSONAL DATA, OBJECTIVES, DOMAIN AND DURATION OF DATA MANAGEMENT

The data management of Data Manager's activities is based on voluntary consent or legal authorization. In the case of data processing based on a voluntary contribution, the data subjects may withdraw their consent at any stage in the processing of data. In some cases, a set of specified data
handling, storing and forwarding are legal, and we will notify our audience separately. We are kindly advising the Data Handler to inform the data providers that, if they do not provide their personal information, the obligation of the data supplier is to obtain the consent of the person concerned. The communicator assures you that it is
for the treatment of personal data made or made available to him by other natural persons, the consent of the natural person concerned is legitimately acquired

3.1. Cookie managemen at www.coolfire.hu

In order to provide customized service, the Data Manager has a small data packet on the user's computer, place a cookie and read it later. If the browser returns a previously saved cookie, the cookie operator can link the user's current visit but only for its own content. Cookies can be deleted from your computer or disabled in your browser. To manage your cookies, you can usually use cookies, or cookies in the Tools / Preferences menu in the Privacy / History / Custom Settings menu tracking is possible. Possible consequences of failure to provide data: unavailability of the services of the website, inaccuracy of analytical measurements.

"Usage supplier cookies"

These "cookies" allow the www.coolfire.hu website to note how the user chooses the mode of operation (eg website uses Hungarian, German or English versions, selects the barrier-free version, how many hits are displayed in the search results list at one time, etc.). This is done in order,
so that you do not have to re-enter them at the next visit.

"targeted ad cookies"

The purpose of using "targeted ad cookies" is to select the ads most relevant to or relevant to the user and appear on our site. These cookies allow third-party service providers, including Google, to display targeted ads on other sites that the user uses, based on a user's visit on a user's site.

These cookies do not even know the user personally. However, the page that the user visited, the page where he clicked, how many pages he opened.

For more information on Google Advertising Privacy Policy, please visit this link:
http://www.google.com/intl/hu/policies/technologies/ads/

The website uses the "targeting and advertising cookies" of the following providers:

- Google Adwords: Detailed information about this service can be accessed via the following link: https://www.google.com/intl/en/policies/privacy
- Facebook: Detailed information on the service can be accessed via the following link: https://www.facebook.com/help/cookies/
- Doubleclick: Detailed information about this service can be found at https://www.google.com/intl/en/policies/privacy
- Sizmek: Detailed information on this service can be found at the following link: http://www.youronlinechoices.com/uk/faqs#15

"web stats cookies"

The Data Manager uses "web statistics cookies" to collect information about how users use the site. The purpose of using cookies is to improve the website's user-friendliness. Using "cookies", you can track how many people visit the site and what content they are interested in.

The site uses Google Tag Manager, Google Analytics analytical cookers, which collect information about how users use the site. This service information is available via the following link: https://www.google.com/analytics/terms/us.html

The purpose of the data management is to identify, distinguish between users, identify users' current session, store data, prevent data loss, web analytics, monitor the functioning of the website, prevent abuses, and measure user needs.

Legal Basis for Data Management: GDPR Article 6. (a), the consent of the person concerned, and Eker. TV. 13 / A. (3) and GDPR Article 6 (1) (f).

Data managed: date, time, IP address, page of previously visited page, user operating system and browser data, time spent on the page. Data management duration: 30 days after viewing the site, except for session cookies that are automatically deleted by leaving the web site or closing the browser.

The portal html code contains references to external servers and external servers independent of the Data Manager. The external service providers are connected directly to the user's computer. We are reminded that the providers of these links are direct linking to their server, user data (eg IP address, browser, operating system data, mouse pointer movement, clicks, visited page title and time and date of visit) due to direct communication with the user's browser) are able to collect. The IP address is a series of numbers that can be clearly identified by the computers and mobile devices of users on the Internet. IP addresses can also geographically locate a visitor using that computer. The addresses of the pages visited, as well as the date and time data are not suitable for identifying the person concerned, but are linked to other data (such as those provided during registration) to help draw conclusions about the user.

Some parts of the portal are used by our partner, Google's reCAPTCHA, robots. Google can provide information about data management with user control: https://www.google.com/intl/en/policies/

The Data Controller shall forward the data for the purpose of providing IT background services to the C-Host Ltd. hosting provider.

Hosted by:
C-Host Ltd. (Nethely.hu); 1115 Budapest, Halmi street 29.
Email: info@nethely.hu
Tel: +36 1 445 20 40
Fax: +36 1 445 20 38

3.2. Contact
If you are looking for the Data Manager for the services that you provide, you can contact us via the contact details provided in this Prospectus or on the website.

The purpose of data management: business continuity.
The legal basis for data handling is the consent of the data subject and the legitimate interest of the data controller: business continuity. Article 6 (1) (a) and (f) of the GDPR and Infotv. Article 5 (1).

The range of managed data is: name, e-mail address, company, phone number, date and time of signing, IP address, date and time of some interactions (openings, clicks, feedbacks, responses, unsubscriptions). Data Handling Duration: The Data Handler deletes all emails received with the sender's name, e-mail address, date, time, and other personal data specified in the message, up to 90 days after the date of communication. If contact is considered a consumer complaint
It takes a data record and records the complaint with a copy for 5 years. TV. 17 / A. (7) of the Act.

We use the Google reCAPTCHA feature in the so called. robots. Google can provide information about data management with user control: https://www.google.com/intl/en/policies/

The Data Controller transmits the data to the C-Host Ltd. (Nethely.hu); 1115 Budapest, Halmi utca 29 hosting provider.

3.3. Electronic Newsletter
The Data Manager will regularly inform your customers and prospective customers of your products and promotions through newsletters. In the newsletter, subscribers will be informed about the products and actions of the Data Manager and other useful information at intervals (eg monthly and half-yearly). Newsletters may also contain advertising messages.

The purpose of the data management is to send electronic newsletters containing commercial advertisement to the interested parties, providing information on current information, events and offers. Legal Basis for Data Processing: GDPR Article 6 (1) (a); the voluntary contribution of the concerned, Infotv. Article 5 (1).

In any case, the Data Controller provides the opportunity to make any further use or consent of the data subject forbidden for this purpose at any time, without limitation and without justification, modify or withdraw it freely. The Data Operator is entitled to access the data of a non-natural person for these purposes until explicitly blocked.

A Contribution Statement can be made in any way that includes the name and email address of the declarant and the scope of the personal data that the contributor agrees to deal with and the voluntary disclosure of the consent with the appropriate information. Any interested party can make an express consent statement in any format.

The range of data to be handled is: e-mail address, date and time of subscription, IP address, this is the date and time of certain interactions (openings, clicks, feedbacks, responses, unsubscriptions, etc.).

Duration of data handling: until the consent statement is withdrawn.

The affected party may, without limitation and justification, modify or withdraw the declaration that contributes to the data handler at the Data Manager. You can do this by following the customer's request:

- at the customer service of the Company personally by completing and signing a statement;
- the completed and signed declaration by post to the registered office of the Company (1149 Budapest, Kövér Lajos u. 31-37.);
- through our telephone support team at + 36-20-283-9404;
- by unsubscribing the "unsubscribe option" link at the bottom of the email received electronically;
- via email at info@coolfire.hu.

Counterfeiting by customers should not apply to business correspondence and information activities arising from the normal course of business, information and provision of information about the client's contract.
The Data Controller transmits the data to the C-Host Ltd. (Nethely.hu); 1115 Budapest, Halmi utca 29 hosting provider.
The Data Controller does not provide third parties with any advertising purpose or make personal data available.

3.4. Further data management
Data management not listed in this information is provided when data is included.

IV.
STORAGE OF PERSONAL DATA, SAFETY OF DATA MANAGEMENT

Data management computer systems and other data retention locations are located at the head office and data processors.
The Data Controller selects and manages the IT tools used to manage personal data and provide the service so that the data processed

a) has been granted access to (availability)
b) credibility and authentication (authenticity of data management)
c) can be verified (data integrity)
d) unauthorized access (confidentiality of data).

The Data Controller protects the data by appropriate measures, in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as accidental destruction, damage and any unavailability of the technology used. The Data Controller ensures, by means of an appropriate technical solution, that the stored data - unless permitted by law - can not be directly linked and assigned to the data subject in order to protect electronically managed files in their various registers. In view of the technical state of the art, the Data Controller provides technical, organizational and organizational measures to protect the security of the data management that is related to the data handling risks provides an adequate level of protection.

The Data Manager retains the data handling

a) confidentiality: it protects the information so that it can only be accessed by those who are entitled to it;
b) integrity: it protects the accuracy and completeness of information and processing methods;

c) Availability: Ensure that when the eligible user needs it, you really have access to the information you need and have the tools available to you.
d) The Data Management and Partner's IT system and network are protected against computer-aided fraud, espionage, sabotage, vandalism, fire and flood, as well as computer viruses, computer burglaries, and denial-of-service attacks. the operator provides security with server-level and application-level security procedures.

Let us know that electronic mails transmitted over the Internet are vulnerable to network threats that lead to unfair practices, controversy or disclosure or modification of information. In order to protect such threats, the Data Controller will take all the precautionary measures he or she may have to take. Systems are monitored to capture all security dangers and provide evidence of any security incident. The system monitoring also allows checking the effectiveness of the precautions applied.

In the event of a privacy incident, the Data Controller shall, without undue delay and, if possible, 72 hours after the data protection incident becomes known, notify the competent supervisory authority under Article 55 unless the data protection incident is unlikely to pose a risk to natural persons rights and freedoms. If the notification is not filed within 72 hours, the reasons for proving the delay must also be enclosed.

If the privacy incident is likely to pose a high risk to the rights and freedoms of natural persons, the data controller shall inform the data subject of the data protection incident without undue delay. The person concerned shall not be informed if any of the following conditions are met:

- the Data Operator has implemented appropriate technical and organizational protection measures and applies these measures to data covered by the data protection incident, in particular measures such as the use of encryption to access personal data make data untitled to unauthorized persons;
- the Data Controller has taken further measures following the data protection incident to ensure that high risk for the rights and freedoms of the person concerned is no longer likely to be realized;
- the information would require disproportionate effort. In such cases, the data subject shall be informed by means of publicly disclosed information or a similar measure shall be taken to ensure that such information is equally effective.

If the Data Controller has not yet informed the data subject of the privacy incident, the supervisory authority may, after considering whether the privacy incident is likely to pose a high risk, may inform the data subject.

The site may include links to or from websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these have their own privacy policies and are not responsible for these policies.

Please review these policies before sharing any personal information with these websites.

Keep in mind that any content published on any of our social media platforms is visible to the public, so please be cautious about providing certain personal information, such as financial information or address information. We will not be responsible for any other act of any other person if you are publishing your personal information on a social media platform and at the same time suggest that you do not share such information.

V.
ADAPTATION, DATA PROCESSING, EXTERNAL SERVICE PROVIDERS

5.1. General principles

We inform our clients that information, data transmission, transfer of data and other information from other bodies are authorized by the court, the prosecutor, the investigating authority, the offender authority, the administrative authority, the National Data Protection and Information Authority, the National Bank of Hungary, you can search the Data Handler for access to documents.

The Data Controller shall, to the extent that the authority indicates the precise purpose and scope of the data, issue personal data only to and to the extent strictly necessary for the purpose of the request.
The Data Controller shall not transfer the personal data it manages to the data processors specified in this prospectus and to third parties other than external providers. Exceptions to the provision in this section are the use of data in a statistically aggregated form that can not otherwise contain any other data capable of identifying the data subject concerned, which does not constitute data management or data transmission.

Transmission of data to processors specified in this Prospectus may be carried out without the specific consent of the person concerned. Issuance of personal data to a third party or authorities may, unless otherwise provided by law, be made solely on the basis of an official decision or at the express prior consent of the person concerned.

5.2. Data processors
For the purposes of performing the activities of the Data Controller, it is necessary to use the data processors named in this Prospectus. The processors will not make a stand-alone decision, only the contract with the Data Manager and the right to proceed with the instructions received. After processing the data processors on May 25, 2018 by the Data Controller personal data transmitted and processed or processed are recorded, processed or processed in accordance with the provisions of the GDPR. and make a statement to the Data Controller. The Data Controller checks the work of data processors. Data processors are only entitled to use a data processor with the consent of the Data Manager.

Hosted by:
C-Host Ltd. (1115 Budapest, Halmi street 29.)
www.coolfire.hu website developer and maintainer:
GlobalWeb Consulting Ltd.
1039 Budapest, Juhász Gyula street 11.

If the Data Handler submits the operation or utilization of the Content Services and Hosting Services to www.coolfire.hu in whole or in part to a third party, the personal data it manages in whole or in part for this third party without requesting the separate consent of the data subject, but the prior information of the data controller you may transfer it to the new operator by reason of the fact that this transfer of data may not render the data communicator more disadvantaged than the data management rules outlined in the current version of this Prospectus. In the case of data transfer under this point, the Data Controller provides the data communicator with the opportunity to object to data transmission before the data is forwarded. In the event of a protest, the transmission of that User's data according to this point is not possible.

5.3. External service providers
The personal data handled by external service providers are governed by the information contained in the third party's own privacy statement. The Data Controller shall do its utmost to ensure that the external service provider manages the personal data transmitted to him in accordance with the law and uses them solely for the purpose specified by the user or for the purposes set out in this Prospectus. After the 25th of May 2018, external service providers record, manage and process personal data transmitted and processed or processed by data controllers in accordance with the provisions of the GDPR, and make a statement to the data controller.

Third party service facilitators: The Data Controller cooperates with third-party service providers for providing services to provide users with registration and access applications. Within this cooperation, some personal data (eg IP address, e-mail, registration name) may be transferred to the data controller and / or data processor by external service providers. These external service providers collect, manage and transmit personal data according to their own privacy policy.

An external service provider that cooperates with the data handler to register or access: Facebook Inc.

Webanalitical and ad server external service providers
Related to the pages of services, the data handler works with webanalytics and ad serving external service providers. These third-party service providers may have access to the user's IP address, and in many cases

cookies, sometimes web beacons (IP address, Web tag for web pages, occasionally e-mail or mobile apps), clicktag (one they provide the services with the use of markup metric code identifying clicks on a given ad) or other click metrics personalization or analysis, and the production of statistics.

Cookies placed by these third-party vendors can be deleted from the user's device at any time, and by choosing the appropriate settings for the browser (s), you can generally refuse the use of cookies. The cookie placed by external service providers can be identified based on the domain associated with that cookie. Rejection of web beacons, clicktags, and other click metrics is not possible. These external service providers treat the personal data transmitted to them by their own privacy policy.

Outsourcing service providers and weblogs that work with the data handler: Facebook Inc., Google LLC.

Third party providers providing customized messaging:
The data controller cooperates with an external service provider that allows the user to access certain services that he or she is using within the same services as other channels (such as Facebook, Messenger, Viber, etc.) used by the same user. The external service provider may use additional cookies, questionnaires and user registration on the website or interfaces of the external service provider to collect additional information about the User that can either be individually or in combination with other data to identify the user. These external service providers treat the personal data transmitted to them by their own privacy policy.

Other external service providers
There are some external service providers with which the data controller is not in a contractual relationship or intentionally does not cooperate with that data management but still have access to the website / services and thus collect data on users or on site activities that they occasionally - independently or individually - connected with the data collected by this external service provider - can be useful for identifying the user. Such external service providers may, in particular but not limited to: Facebook Ireland LTD., Google LLC, Instagram LLC., Twitter International Company, Viber Media LLC, Vimeo Inc., YouTube LLC. These third party service providers treat personal data transmitted to them according to their own privacy policy.

VI.
THE RIGHTS OF THE INTERESTED PARTIES

6.1. The User may request that any Data Manager informs you that you are handling the personal data of the person concerned and, if so, you will have access to the personal information you are managing. You may request information on the handling of personal data provided by the data subject in writing by registered mail or by e-mail addressed to this e-mail address sent by registered mail to the address of the Data Handler referred to in point I of this Information. The information request sent by letter is deemed to be authentic by the Data Manager if the request is sent to the person who is clearly identifiable. The information handler sent by e-mail will only be considered credible if it is sent from the given e-mail address, but this does not preclude the Data Manager from identifying the User before providing the information. The request for information may cover the data of the data subject managed by the Data Controller, their source, the purpose, legal basis, duration of the data processing, the names and addresses of the data processors, data management activities and, in the case of the transfer of personal data, who and for what purpose information about the person concerned.

6.2. The person concerned may request correction or modification of the personal data handled by the Data Controller. Taking into account the purpose of the data handling, the data subject may request the supplementation of incomplete personal data as specified in section 6.2.

6.3. The person concerned may request the deletion of personal data handled by the Data Controller. Cancellation may be refused (i) for the purpose of exercising the right to freedom of expression and access to information, or (ii) where it is authorized by law to handle personal data; and (iii) submitting, enforcing, or protecting legal claims. In any case, the Data Handler informs the person concerned of the denial of the cancellation request, indicating the reason for the denial of cancellation. After the request for deletion of personal data, previous (deleted) data can no longer be recovered.

Newsletters sent by the Data Manager can be retrieved via the unsubscribe link. In the event of unsubscribe, the Data Handler will delete the relevant personal data in the newsletter database.

6.4. An individual may request that his or her personal data is handled by the Data Controller if the person concerned disputes the accuracy of the personal data he handles. In this case, the restriction refers to the time period in which the Data Controller checks the accuracy of the personal data. The Data Controller shall indicate the personal data he or she handles if the person concerned disputes its correctness or accuracy, but the incorrect or imprecise nature of the disputed personal data can not be clearly identified. An individual may request that his or her personal data is handled by the Data Controller even if the data handling is illegal but the party concerned opposes the deletion of the personal data processed and instead requests that they be restricted. The data subject may also request that the processing of his or her personal data is restricted by the Data Controller if the purpose of the data processing is achieved but the data subject requires their Data Management to handle, enforce, or protect legal claims.

6.5. An interested party may request that the Data Handler hand over and / or transfer data transmitted to the data subject by the data subject and processed by the data subject in an automated manner in a machine-readable format widely used and / or transferred to another data controller.

6.6. The person concerned may object to the handling of his or her personal data (i) if the processing of personal data is only necessary to comply with a legal obligation for data controllers or to enforce the legitimate interests of the Data Controller or third party; (ii) where the purpose of data processing is to direct business acquisition, polling or scientific research; or (iii) if the data is processed in order to perform a public interest task. The Data Controller examines the lawfulness of the victim's protest and, if it establishes the grounds for the protest, terminates the processing of data and locks the personal data processed, and notifies the protest and the measures taken on the basis of those who have previously been transferred to the personal data affected by the protest.

VII.
Data Audit

The Data Manager keeps the user's personal data only as long as he or she needs the purpose for which he / she stores his / her personal data to meet the user's needs or to comply with his / her legal obligations.
Data that is automatically recorded in the system during the operation of the system will be stored in the system for a reasonable period of time from the time of their generation to ensure that the system operates. The Data Controller ensures that these, automatically recorded data with other personal data - the law except in cases that are mandatory.

In order to comply with certain legal or regulatory obligations and to allow our company to manage our rights (for example, enforcing our court claims) or for statistical or historical purposes, some personal data may be retained. If we no longer need to use your personal information, we will be removed from our systems and records or anonymised to the extent that your identity can no longer be identified.

VIII.
MODIFICATION OF THE DATA SHEET INFORMATION

The Data Controller reserves the right to modify this Prospectus at any time by its unilateral decision. By entering the next entry, you agree to the applicable provisions of this Prospectus, and there is no need to seek the consent of any individual.

IX.
JUSTICE OPPORTUNITIES

You can search for any data-related questions and observations in the Data Handler's e-mail address given in point I of this Prospectus.
The data subject directly complains to the National Data Protection and Information Authority (1125 Budapest, Szilágyi Erzsébet fasor 22 / c, phone: + 36-1-391-1400;
e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu).

In case of violation of the rights of the concerned person, he or she may appeal to the court. The trial is governed by the jurisdiction of the court. The case may be initiated before the tribunal of the domicile or place of residence of the person concerned, according to his choice. The Data Handler informs the person concerned of the opportunity and means of remedies on request.

Budapest, May 24, 2018