

Data Protection and Privacy Notice

I. Introduction

This Data Protection and Privacy Notice (the 'Notice') aims to record the data protection and data processing principles related to the web shop available at **artypical.hu and artypical.store** (the 'Website') operated by **Lime Creative Kft** (the 'Company'), so the data subjects can receive appropriate information about the data managed and processed by the Company – and the Data Processors engaged by it – their source, the purpose, legal basis and duration of data processing, the name and address of the Data Processor that may be involved in data processing and its activities related to data processing, as well as, if the data subject's personal data are transmitted, the legal basis for and recipient of such data transmission.

II. Applicable legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR);

- Act CXII of 2011 on informational self-determination and freedom of information;
- Act V of 2013 on the Civil Code (the 'Civil Code');
- Act C of 2000 on accounting (the 'Accounting Act');
- Act XLVIII of 2008 on the basic conditions of, and certain restrictions on, commercial advertising activities;
- Act CXIX of 1995 on the processing of name and home address data serving the purposes of research and direct marketing;
- Act XLVII of 2008 on the prohibition of unfair commercial practices vis-à-vis consumers;
- Act CVIII of 2001 on certain issues of electronic commerce services and information society services;
- Act CL of 2017 on tax procedures (the 'Tax Procedures Act').

III. Definitions

The conceptual system of this Notice corresponds to the interpretative definitions set out in Article 4 GDPR, in particular:

- 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- 'data processing' means the performance of technical tasks associated with the processing operations of personal data, whether or not by automated means, irrespective of the means and method used for carrying out the operations and

the location of such use, provided that the technical task is performed on the data;

- 'data processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;
- 'data controlling' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- 'data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- 'data transmission' means the transmission of processed personal data to other Data Controllers for purposes other than data processing; 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
 - 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to identified or identifiable natural persons;
 - 'consent of the data subject' means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
 - 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law should not be regarded as recipients; the processing of those data by those public authorities should be in compliance with the applicable data protection rules according to the purposes of the processing;
 - 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
 - 'special data' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic and biometric data for the unique identification of natural persons, health data and personal data concerning the sexual life or sexual orientation of natural persons;

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

If the definitions of the GDPR in force at any given time differ from the definitions in this Notice, the definitions given in the Regulation prevail.

IV. Principles of data processing

4.1 Principles of legality, due process and transparency

Personal data must be processed lawfully and fairly and in a transparent manner in relation to the Data Subject. In the interest of lawful data processing, it must be based on the consent of the Data Subject or must have another basis established by law.

Personal data may be processed only if the purpose of data processing cannot reasonably be fulfilled by other means.

Any information and communication relating to the processing of personal data must be easily accessible and easy to understand, and clear and plain language must be used.

In order to achieve fair, transparent data processing, it is necessary that the Data Subject is informed about the fact and purposes of data processing.

If the Company collects personal data directly from the Data Subject, it is necessary to inform the Data Subject whether they are obliged to disclose the personal data and what consequences non-disclosure may have on them. The information must be provided to the Data Subject at the time of data collection.

If the data were collected from sources other than the Data Subject, the information must be made available to the Data Subject within a reasonable time. If the personal data can be lawfully disclosed to another recipient, the Data Subject must be informed about it at the time of the first disclosure.

The obligation to provide information is not necessary if the Data Subject already has this information or if the recording or disclosure of personal data is expressly provided for by legislation or if the provision of information to the Data Subject proves impossible or required a disproportionately large effort.

The Data Subject must ensure that they receive access to their personal data processed by the Company free of charge, request their rectification or erasure, and exercise their right to object. The Data Controller is obliged to respond to the request of the Data Subject without undue delay, but no later than within 25, say twenty-five, days, or if the Data Controller does not comply with any request of the Data Subject, it must justify it.

4.2. Purpose limitation principle

Personal data may only be collected for a specific, clear and lawful purpose. It is prohibited to process personal data in a way that is incompatible with their purposes.

The processing of personal data for purposes other than the original purpose for which they were collected is permitted only if data processing is compatible with its original purposes for which the personal data were originally collected. In this respect, it is necessary to examine, in particular, but not limited to, the relationship between the original and intended purposes of data processing, the circumstances of data collection and the nature of the personal data.

4.3. Principle of data minimisation

The processing of personal data must be appropriate and relevant for the purposes and the processing of personal data must be limited to the necessary minimum.

In order to ensure the implementation of the principle, the Data Controller must implement appropriate technical and organisational measures, such as pseudonymisation, both in determining the way in which the data are processed and in the data processing process, with the aim of, firstly, implementing the data protection principles and, secondly, incorporating the guarantees necessary for the protection of the rights of the Data Subjects into the data processing process.

The Data Controller is obliged to implement technical and organisational measures that ensure that only personal data necessary for the specific purpose of data processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the duration of their storage and their accessibility.

4.4. Principle of accuracy

The personal data collected, stored and processed by the Data Controller must be accurate and, if necessary, up-to-date. The Data Controller must take all reasonable measures to forthwith erase or rectify personal data that are inaccurate for the purposes of data processing.

In order to ensure the implementation of the principle of accuracy, the Data Controller is obliged to verify the accuracy of the data (right to rectification and erasure) in the event of a request made to that effect by the Data Subject and, if necessary, to modify and erase the specified personal data.

4.5. Principle of storage limitation

In order to ensure the implementation of the purpose limitation principle, it must be ensured, in particular, that the period for which the personal data are stored is limited to a strict minimum. In order to ensure that the personal data are not kept longer than necessary, the Data Controller must set deadlines for erasure or for a periodic review.

Personal data must be stored in such a way that the identification of the Data Subject can only be possible for the time necessary to achieve the purposes for which the personal data are processed. Personal data may be stored for a longer period only if their processing is for archiving purposes in the public interest, for scientific and historical research, or for statistical purposes.

4.6. Principle of integrity and confidentiality

Personal data must be processed in a manner that ensures their appropriate security and confidentiality, including for preventing unauthorised access to or use of personal data and the equipment used for their processing.

In order to ensure the implementation of the principle, the Data Controller must use technical or organisational measures during the processing of personal data to ensure that the security of the personal data is satisfactory throughout. In this respect, it is necessary to also provide protection against the unauthorised or unlawful processing, accidental loss or destruction of or damage to the data.

4.7. Accountability of the Data Controller

The Data Controller is obliged to comply with the principles detailed above and to be able to prove compliance during the processing of personal data.

V. Rights of the Data Subject

The Data Subject may exercise their rights in the following ways:

- **by e-mail:** webshop@artypical.hu
- **by post:** Lime Creative Kft 1112 Budapest, Budaörsi út 163B

5.1 Right of access

At the request of the Data Subject, the Data Controller provides information on whether their personal data are being processed; if so, it should grant access to the Data Subject.

5.2 Right to rectification

At the request of the Data Subject, the Data Controller corrects any inaccurate personal data relating to the Data Subject or supplements any incomplete data without undue delay.

5.3 Right to erasure

At the request of the Data Subject, the Data Controller erases the relevant personal data without undue delay if one of the following reasons exists:

- if the purpose of data processing has ceased to exist or if its statutory deadline has expired;
- if the Data Subject revokes their consent and there is no other legal basis for data processing;
- if the Data Subject objects to data processing and there is no priority legitimate reason for it;
- if the data processing is unlawful;
- if the personal data are incomplete or incorrect, and this condition cannot be remedied lawfully;

- it needs to be erased pursuant to the provisions of legislation;
- if ordered by an authority or the court.

In the event that the Data Controller has disclosed the personal data which it has to erase on the basis of the above, it is obliged to take all measures to inform the other Data Controllers of the obligation of erasure, as far as possible (state of the art and implementation costs).

The personal data need not be erased even in the case of the above reasons for erasure if data processing is necessary for one of the following reasons:

- for exercising the right to freedom of expression and information;
- for compliance with a legal obligation which the Data Controller is subject to or performing a task in the public interest assigned to the Data Controller;
- no health data specified in legislation may be erased for the purpose of a public interest in public health;
- for archiving in the public interest, for scientific and historical research purposes, or for statistical purposes, where erasure would be likely to render impossible or seriously jeopardise data processing;
- required for the submission and enforcement of legal claims or for indictment.

5.4 Right of restriction of processing

At the request of the Data Subject, the Data Controller restricts the processing of their personal data if one of the following conditions is fulfilled:

- the Data Subject disputes the accuracy of their personal data (in this case, the restriction applies to the period that allows the Data Controller to verify the accuracy of the personal data);
- the Data Controller no longer needs the personal data of the Data Subject, nonetheless, it requires them for submitting, enforcing or protecting legal claims;
- the Data Subject has objected to data processing; in this case, the restriction applies to the period that allows the Data Controller to examine whether the legitimate interests of the Data Controller take precedence over the legitimate reasons of the Data Subject.

During the restriction of data processing, it must be ensured that no data processing operation can be carried out on personal data. During the restriction of data processing, personal data may only be processed by the Data Controller, except for storage, with the consent of the Data Subject or for submitting, enforcing or protecting the legal claims of the Data Controller or for protecting the rights of other natural or legal persons or out of important public interest of the EU or a Member State.

In the event of a restriction of data processing, the Data Controller informs the Data Subject in advance of its lifting.

5.5 Right to object

The Data Subject is entitled to object at any time to the processing of their personal data by the Data Controller if its legal basis is the exercise of rights in the public interest or the prerogatives of a public authority conferred on it or the enforcement of the legitimate interests of the Data Controller or a third party. The Data Subject may also exercise the right to object by automated means based on technical specifications by unsubscribing from the newsletter.

5.6 Right to data portability

The data subject is entitled to receive the personal data related to them and provided by them to a Data Controller in a structured, commonly used and machine-readable format and to transmit such data to another Data Controller without being hindered by the Data Controller to which it has provided the personal data.

5.7 Right of revocation

The Data Subject is entitled to revoke their consent to the processing of their personal data by the Data Controller at any time. The revocation of consent does not affect the lawfulness of data processing based on consent before such revocation. After the revocation of consent, the Data Controller is obliged to delete the personal data processed on the basis of such consent.

5.8 Right of remedy of the Data Subject

In the event of a complaint about data processing, if you have any requests or questions about data processing, you can send your inquiry by post to the registered office of the Data Controller or electronically to the e-mail address indicated at the contact details of the Data Controller. We will send our answers without delay, but within no more than 30 (thirty) days to the address you requested.

The Data Subject is entitled to lodge a complaint with the National Authority for Data Protection and Freedom of Information without prejudice to other administrative or judicial remedies if they consider that the Data Controller has violated the provisions of law during the processing of their personal data (for example, unlawful processing, disagreement with a decision on data processing or information provided by the Data Controller, late provision of data or omission by the Data Controller).

National Authority for Data Protection and Freedom of Information	
Mailing address:	1363 Budapest, Pf. 9.,
Hungary address:	1055 Budapest, Falk Miksa utca 9-11., Hungary
Telephone:	+36-1-391-1400
Fax:	+36-1-391-1410

e-mail:	ugyfelszolgalat@naih.hu
website:	http://naih.hu/

A judicial remedy is available against the decision of the supervisory authority.

The Data Subject is entitled to initiate proceedings with the court to remedy the infringement sustained if the Data Controller does not process their personal data in accordance with legislation. The Data Controller is obliged to compensate the Data Subject for pecuniary and non-pecuniary damages caused by unlawful data processing. The adjudication of data protection lawsuits falls within the competence of the regional court. The Data Subject may also file a lawsuit, at their option, before the regional court with jurisdiction at their domicile of residence.

The list of regional courts (name and contact details) and the jurisdiction search service are available on the www.birosag.hu website.

If their rights related to content that insults minors, incites hatred or is exclusionary, corrections, the rights of a deceased person or the violation of good reputation are infringed, the Data Subject may initiate proceedings with the National Media and Communications Authority.

National Media and Infocommunications Authority	
mailing address:	1525 Pf. 75.
Hungary address:	1015 Budapest, Ostrom utca 23-25., Hungary
Telephone:	+36-1-457-7100
Fax	+36-1-356-5520
e-mail:	info@nmhh.hu
website:	http://nmhh.hu

In the event that the Data Controller infringes the personality rights of the Data Subject by unlawfully processing their data or violating the data security requirements, the Data Subject may demand an injury fee from the Data Controller.

VI. Data Controller and its contact details

The Data Controller is obliged to implement appropriate technical and organisational measures to ensure and demonstrate that personal data are processed in accordance with data protection legislation, taking into account the nature, scope, circumstances and purposes of data processing and the risk to the rights and freedoms of natural persons, with a varying probability and severity. At all stages of data processing, it is required to comply with the purpose of data processing and the relevant legal rules.

The technical and organisational measures applied for lawful data processing are reviewed and, if necessary, updated by the Data Controller.

In connection with the data provided, the Data Controllers are as follows:

Name:	Lime Creative Kft
Registered office:	1112 Budapest, Budaörsi út 163B
Company register No:	01-09-916681
Tax No:	14719385-2-43
Represented by:	Buday Tímea
e-mail address:	webshop@artypical.hu

VII. Data processor and its contact details

If data processing is carried out by someone else on behalf of the Data Controller, the Data Controller may only use Data Processors who or which provide appropriate guarantees for the implementation of appropriate technical and organisational measures to ensure compliance by data processing with legislation and the protection of the rights of the Data Subjects.

If a Data Processor is used, the ultimate responsibility remains with the Data Controller, who must supervise the Data Processors in order to ensure that their decisions comply with data protection legislation.

VIII. Data protection officer and their contact details

Pursuant to Article 37 GDPR, the Data Controller is not obliged to appoint a data protection officer.

IX. Process of data processing

The data may be processed by the staff of the Data Controller only to the extent essential for performing their tasks if the Data Controller employs staff. If it does not employ any staff, the data will be processed by the representative of the Data Controller.

Please note that the Data Controller does not perform any data processing activity in connection with the functions invited by the shortcuts of external service providers (Facebook, Twitter, LinkedIn and Instagram) appearing on the website. In these cases, the data controller is the third party company providing the service.

9.1. Newsletter and direct marketing activities, social media sites

Subscribing to the newsletter is based on voluntary consent.

<p><i>Name, description and purpose of data processing</i></p>	<p><i>Sending out newsletters</i></p> <p><i>When subscribing to the newsletter, we are not in a position to verify the authenticity of the contact details and to establish that the details provided relate to an individual or business. We treat companies that contact us as customer partners.</i></p> <p><i>The purpose of data processing is to send professional brochures, electronic messages containing advertisements, information and newsletters, from which you can unsubscribe at any time without consequences. You can also unsubscribe without any consequences if your business has in the meantime ceased to exist, you have left the business, or someone has provided us with your contact details.</i></p> <p><i>We may send you a newsletter if you consent in advance and expressly (during registration and by filling in the name, e-mail address and consent checkbox when subscribing to the newsletter) to us providing you with our advertising offers, information and other items at the e-mail address provided during registration. As a result, you may consent to us processing your personal data necessary for this purpose. In accordance with the above, if you wish to receive a newsletter, you must provide the necessary details. If you do not provide the details, we will not be able to send you the newsletter.</i></p>
<p><i>Scope of Data Subjects</i></p>	<p><i>Those subscribing to the newsletter</i></p>
<p><i>Legal basis for data processing</i></p>	<p><i>Your consent.</i></p>

<i>Scope and purpose of the processed data</i>	<i>Last name</i>	<i>identification, contact and sending newsletters</i>
	<i>First name</i>	<i>identification, contact and sending newsletters</i>
	<i>E-mail address</i>	<i>identification, contact and sending newsletters</i>
<i>Duration of data processing and erasure of data</i>	<i>The data are processed until consent is revoked. The data will be deleted when the consent to the data processing is revoked. You may revoke your consent to data processing at any time by using the unsubscribe link in the newsletters sent to you.</i>	
<i>Who can have access to the personal data?</i>	<ul style="list-style-type: none"> ● <i>authorised staff of the Data Controller</i> 	
	<ul style="list-style-type: none"> ● <i>authorised staff of the Data Processor</i> 	
<i>Method of data storage</i>	<i>electronic</i>	

9.2 Complaints management

Lodging a complaint is based on voluntary consent, but pursuant to the data processing legislation (Act CLV of 1997) it is mandatory in respect of the processed data.

<i>Name, description and purpose of data processing</i>	<i>Complaints management You may report your complaint about the service or product or the conduct, acts or omissions of the Data Controller in writing (by post or e-mail). The purpose of data processing is to identify the Data Subject and the complaint as well as to record the data that are mandatory to be recorded from the law, as well as to enable the communication of the complaint and to maintain contact.</i>
---	--

<p><i>Scope of Data Subjects</i></p>	<p><i>Every natural person who wishes to report a complaint about the service or the conduct, acts or omissions of the Data Controller in writing.</i></p>	
<p><i>Legal basis for data processing</i></p>	<p><i>The complaint handling process starts on the basis of voluntary consent, but in the case of a complaint it is mandatory pursuant to the legislation on data processing (Act CLV of 1997).</i></p>	
<p><i>Scope and purpose of the processed data</i></p>	<p><i>Complaint ID</i></p>	<p><i>identification</i></p>
	<p><i>Place, time and manner of receipt of the complaint</i></p>	<p><i>identification</i></p>
	<p><i>E-mail address</i></p>	<p><i>identification, liaison</i></p>
	<p><i>Personal data provided by e-mail</i></p>	<p><i>identification</i></p>
	<p><i>Last name</i></p>	<p><i>identification</i></p>
	<p><i>First name</i></p>	<p><i>identification</i></p>
	<p><i>Mailing address</i></p>	<p><i>liaison</i></p>
	<p><i>Subject-matter of complaint</i></p>	<p><i>complaints management</i></p>
	<p><i>Content of complaint</i></p>	<p><i>investigation of complaint</i></p>

	<i>Attached documents</i>	<i>investigation of complaint</i>
	<i>Reason for complaint</i>	<i>investigation of complaint</i>
<i>Duration of data processing and erasure of data</i>	<i>The Data Controller retains the record of the complaint and a copy of the response for 5 years from their date pursuant to Section 17/A(7) of the applicable Act CLV of 1997 in force.</i>	
<i>Who can have access to the personal data?</i>	<ul style="list-style-type: none"> ● <i>authorised staff of the Data Controller</i> 	
	<ul style="list-style-type: none"> ● <i>authorised staff of the Data Processor</i> 	
<i>Method of data storage</i>	<i>electronic, paper-based</i>	

9.3 Request of information

The request for information is based on voluntary consent.

<i>Name, description and purpose of data processing</i>	<p><i>Request of information</i></p> <p><i>You can ask questions about the service or the conduct and activities of the Data Controller in writing (by post or e-mail). The purpose of data processing is to provide the Data Subject with appropriate information and to maintain contact.</i></p>
<i>Scope of Data Subjects</i>	<i>Any natural person who contacts the Data Controller and requests information from the Data Controller in addition to providing their personal data.</i>

<i>Legal basis for data processing</i>	<i>In accordance with the purpose of data processing, you voluntarily consent to the Data Controller contacting you through such data in order to clarify or answer the question if you have provided your contact details when the information was requested.</i>	
<i>Scope and purpose of the processed data</i>	<i>Question ID</i>	<i>identification</i>
	<i>Place, time and manner of receipt of the question</i>	<i>identification</i>
	<i>E-mail address</i>	<i>identification, liaison</i>
	<i>Personal information provided by e-mail</i>	<i>identification</i>
	<i>Last name</i>	<i>identification</i>
	<i>First name</i>	<i>identification</i>
	<i>Mailing address</i>	<i>liaison</i>
	<i>Subject-matter of question</i>	<i>complaints management</i>
	<i>Content of question</i>	<i>investigation of complaint</i>
<i>Duration of data processing and erasure of data</i>	<i>Until the goal is achieved.</i>	
<i>Who can have access to the personal data?</i>	<i>authorised staff of the Data Controller</i>	
	<i>authorised staff of the Data Processor</i>	

<i>Method of data storage</i>	<i>electronic, paper-based</i>
-------------------------------	--------------------------------

9.4 Customer satisfaction survey

<p><i>Name, description and purpose of data processing</i></p>	<p><i>Customer satisfaction survey</i></p> <p><i>The Data Controller is committed to providing its services to a high standard. In order to guarantee the supply of Customers and to ensure the quality of the services provided to them, the Data Controller regularly examines the efficiency of its activities and the standard of the services. The Data Controller evaluates the feedback received and integrates the comments the implementation of which contributes to the provision of services to a higher standard and which can be implemented within the framework of its systems used into its internal processes. If the changes also require an amendment to the regulations, it will include them in the next amendment.</i></p> <p><i>The user experience gained during the purchase and the opinion of our Customers are extremely important to us. To this end, after the purchase, the Data Controller will send the Customers a customer questionnaire or a link to it to the e-mail address provided during the purchase.</i></p> <p><i>Expression of an opinion based on the customer questionnaire is voluntary and completely anonymous. We only use the email address to send the customer questionnaire. The Data Controller handles the answers given on the customer questionnaire completely separately and anonymously from the respondent's personal data. The relationship between the responses and the respondent cannot be reconstructed.</i></p>
<p><i>Scope of Data</i></p>	<p><i>Subjects Any natural person who completes the customer satisfaction questionnaire and consents to the data management.</i></p>

<p><i>Legal basis for data processing</i></p>	<p><i>By completing and submitting the customer satisfaction questionnaire, you voluntarily consent to the Data Controller handling your responses given during the customer satisfaction survey and transmitting them to the Data Processors in accordance with the purpose of data processing.</i></p> <p><i>If you wish to revoke your consent to the use of your e-mail address for future customer satisfaction survey questionnaires, you may indicate your intention to revoke it by one of the notification methods set out in Section V.</i></p>	
<p><i>Scope and purpose of the processed data</i></p>	<p><i>Answers to the individual questions of the questionnaire</i></p>	<p>customer satisfaction survey</p>
<p><i>Duration of data processing and erasure of data</i></p>	<p><i>Until the goal is achieved.</i></p>	
<p><i>Who can have access to the personal data?</i></p>	<ul style="list-style-type: none"> ● <i>authorised staff of the Data Controller</i> 	
	<ul style="list-style-type: none"> ● <i>authorised staff of the Data Processor</i> 	
<p><i>Method of data storage</i></p>	<p><i>electronic</i></p>	

9.5. Cookies

For a website to work properly, it is sometimes necessary to place cookies on your computer, as other large websites and internet service providers do.

Cookies are small text files, which a website stores on the computer or mobile device of a user visiting its pages. Cookies allow the website to remember actions and personal settings for a certain time, such as username, language, font size and other custom settings related to the display of the website, so that you do not have to re-enter them each time you visit the website or when navigating from one page to another.

It is possible to maintain and/or delete cookies as desired. Please visit aboutcookies.org for more information. You may delete all cookies stored on your computer and may also disable their installation in most browsers. In this case, however, you may need to make some

settings manually each time you visit the site and you should also be aware that certain features and functions may not work.

9.5.1. The function of cookies

- *collect information about visitors and their devices;*
- *record the individual settings of visitors, which are (may be) used, (e.g. at the time of making online transactions, eliminating the need to enter them again);*
- *facilitate the use of the website;*
- *provide quality user experience.*

In order to provide customised service, a small data packet, a 'cookie', is placed on the user's computer or other device used for browsing and it is read back at a later visit. If the browser returns a previously saved cookie, the service provider processing the cookie has the option to link the user's current visit to previous ones, but only with respect to its own content.

9.5.2. Essential, session cookies

The purpose of these cookies is to enable visitors to fully and seamlessly browse the Website and to use its features and the services available there. This type of cookies remains valid until the end of the session (browsing), and when the browser is closed, this type of cookies is automatically deleted from the computer or other device used for browsing.

9.5.3. Third party cookies (analytics)

The Website also uses the cookies of Google Analytics as a third party. Using Google Analytics for statistical purposes, the Website collects information about how visitors use websites. It uses the data to improve the website and user experience. These cookies also remain on the visitor's computer or other browsing device, in its browser, until they expire or until the visitor deletes them.

9.5.4. Targeting or advertising cookies

The Website uses these cookies, the purpose of which is to display advertisements that are even more interesting and relevant to the visitor. These cookies can be used, for example, to determine the number of times an advertisement is displayed and to assess the efficiency of advertising campaigns. These cookies are usually placed by advertising networks on a specific website, with the permission of the website operator. These cookies record visits to a particular website and share this information with other organisations, such as the advertiser. Typically, targeting or advertising cookies are related to the features provided by the organisation operating the website.

9.6. Additional information

Some of your data, as shown in the table, are also visible to our other users (recipients) to whom you have made them visible. However, this does not constitute either data transmission or data transfer. Other users can only see your data, but may not perform data processing activities other than viewing them, so you may not process third party data either besides viewing them unless they have specifically consented to it, but this is your legal relationship independent of the Data Controller.

By entering the mandatory data and ticking the checkbox, you consent to it being visible to other users according to 'visibility settings' and to the Data Controller processing them for the purpose indicated in the above table.

By entering the data to be provided voluntarily, optionally, you consent to it being visible to other users according to the 'visibility settings' and to the Data Controller processing them for the purpose and time indicated in the above table. It is not necessary to tick the checkbox here, it only needs to be done at the time of registration, while these data can be provided after registration.

The site does not ask for any special personal data. If someone requested this on behalf of the Data Controller, please let us know.

The Data Controller does not transmit data to either EEA or third countries (non-EEA countries).

The Data Controller does not perform profiling.

The Data Controller is responsible for ensuring that the data are up to date and accurate, so we ask you to notify the Company forthwith of any changes in the data.

X. Data security

The Data Controller provides for data security. To this end, it takes the technical and organisational measures and establishes the rules of procedure that are required for the enforcement of the governing legislation and rules of data protection and confidentiality.

The Data Controller protects, through appropriate measures, the data against unauthorised access, alteration, transmission, disclosure, erasure or destruction, and accidental destruction and damage as well as becoming inaccessible as a result of a change in the technology applied.

The Data Controller (also) ensures the enforcement of the data security rules by means of internal regulations, instructions and rules of procedure separate from the Data Protection and Data Security Regulations and this Notice in content and form.

When specifying and applying measures aimed at data security, the Data Controller takes into consideration the current development level of technology and chooses a data processing solution from several alternatives which provides a higher level of protection of personal data unless it would represent disproportionate difficulties.

Within the scope of its tasks related to IT protection, the Data Controller provide, in particular, for:

- measures to protect against unauthorised access, including the protection of software tools and hardware devices and physical protection (access protection, network protection);
- measures to ensure the possibility of restoring data files, including regular backups and the separate, secure processing of copies (mirroring, backup);
- the protection of data files against viruses (virus protection);
- the physical protection of data files and the devices carrying them, including protection against fire, water damage, lightning, other natural forces, and the recoverability of damage resulting from such events (archiving, fire protection).

The Data Controller ensures the proper backup of the IT data and the technical environment of the Website, which it operates with the necessary parameters based on the retention period of each data, thus guaranteeing the availability of the data within the retention period, and will permanently destroy them upon the expiration of the retention period.

It monitors the integrity and functionality of the IT system and the data storage environment with advanced monitoring techniques and continuously provides the necessary capacities. It records events in its IT environment using complex logging functions, thus ensuring the subsequent detectability and legal proof of possible incidents.

We are constantly using a redundant network environment that provides high bandwidth to serve the Website, which securely distributes the loads that occur between our resources.

We guarantee the disaster resilience of our systems as planned and ensure the business continuity and thus the continuous service of our users at a high level with organisational and technical means.

With a high priority, we ensure the controlled installation of security patches and manufacturer upgrades that also ensure the integrity of our IT systems, thus preventing, avoiding and managing attempts to access or damage it by exploiting vulnerabilities.

We regularly inspect our IT environment with security testing, correct any errors or weaknesses found, and consider strengthening the security of the IT system to be an ongoing task.

We have formulated high security requirements for our employees, including confidentiality.

We also ensure that they are met through regular training, and in connection with our internal operations, we strive to operate planned and controlled processes.

Any incidents involving personal data, which are detected by or reported to us during our operations will be investigated in a transparent manner, in accordance with responsible and strict principles, within 72 hours.

Incidents that have occurred are handled and recorded. During the development of our services and IT solutions, we ensure the fulfilment of the principle of built-in data protection. We treat data protection as a priority requirement already in the planning phase.

XI.Data transmission

The Data Controller is entitled to transmit the personal data collected, recorded and organised by it to a third party.

The principles of data processing (for example, the principle of data minimisation, the purpose limitation principle) must be observed throughout the data transmission. During data transmission, it must also be borne in mind that the recipients should also ensure an appropriate level of protection for the personal data of the Data Subject.

The Data Controller may only use a Data Processor who or which provides appropriate guarantees for the requirements set out in the General Data Protection Regulation and implements appropriate technical and organisational measures, which ensure the protection of Data Subjects. The Data Processor is only entitled to transmit personal data if instructed to do so by the Data Controller. Where the obligation to transmit data is required by the law of a Member State under the law of the Data Processor or by the EU law applicable to it, the transmission may take place without the instructions of the Data Controller, but with its prior notification.

XII. Amendment of the Notice

The Company reserves the right to amend this Notice at any time by unilateral decision.

If the Data Subject does not agree with the amendment, they may request the erasure of their personal data at one of the contact details specified in Section V.