

**DATA MANAGEMENT NOTICE  
REGARDING THE USAGE OF ARENIMTEL.COM, ARENIM.COM AND CRYPTTALK.COM WEBSITES**

**Enters into force: July 1, 2020**

The provider of [www.arenimtel.com](http://www.arenimtel.com) and [www.webwithme.com](http://www.webwithme.com) websites (hereinafter referred to as: **Website**), **Arenim Technologies Fejlesztő és Szolgáltató Kft.** (Seat: 1095 Budapest, Lechner Ödön fasor 6.; Company Registration Nr.: 01-09-330669; Tax number: 12904327-2-43; hereinafter referred to as: **Service Provider**) informs the Users about the data processing on the Website as follows, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council, the General Data Protection Regulation (hereinafter referred to as **GDPR**).

**1. Terms**

<b>Service provider</b>	<b>Arenim Technologies Fejlesztő és Szolgáltató Kft.</b> (Company registration number: 01-09-330669; seat: 1095 Budapest, Lechner Ödön fasor 6.) which company operates the Website.
<b>Website</b>	The entirety of the content and services available on <a href="http://www.arenimtel.com">www.arenimtel.com</a> , <a href="http://www.arenim.com">www.arenim.com</a> , <a href="http://www.crypttalk.com">www.crypttalk.com</a> and <a href="http://www.webwithme.com">www.webwithme.com</a> .
<b>Client</b>	Person who entered into an agreement with the Service Provider in connection with the Service, who uses the Service of the Service Provider.
<b>User</b>	Person visiting or browsing the Website, or Client using the Website.
<b>Service</b>	Telephone exchange, call center, telephone line, WebAssistant, Softphone, software development, IT support, IT operation and consultancy service provided by the Service Provider,
<b>WebAssistant</b>	Screen mirroring and sharing service provided by the Service Provider which enables the Client's customer service personnel to see and track on their own screens in real-time exactly what the Client's clients see and do on the website of the Client.
<b>Softphone</b>	Software phone service provided by the Service provider, which can be installed on a computer thus can replace phones.
<b>Call Center</b>	Customer service solution provided by the Service Provider which contains comprehensive call center functions, online management platform, reports and detailed statistics, and which is able to record and archive calls, which has routing, ACD, group and intelligent call handling and web user support functions including mobile, web and safe customer service services.

**2. What is the purpose of the present notice?**

By using the Website and its services, the Service Provider and the User enter into an agreement. In this present data management notice the Service Provider provides detailed information to the Users and Clients regarding the personal data processing on the Website and during the Service, in accordance with the relevant legal provisions. In the course of processing data on the Website, the Service provider is considered a data controller.

The Service provider is considered a data processor in the course of processing data of the Clients and the Clients' clients in connection with the Services provided to the Clients, on behalf and in the name of the Clients. The data controller of these personal data is the Client, which processes data according to its own data management notice. Clients as separate data controllers are obliged to process data in accordance with the relevant legal provisions and to inform their own clients about their data processing in their own data management notice. The Service provider is not liable for the existence, conformity and legality of the Client's data management notice, the Service provider is only liable for its own data processing. The data processing of the Service provider as a processor is the subject of separate data processing agreements.

### **3. What is the purpose of the Website?**

Users can obtain information on the Website regarding the services provided by the Service Provider without registration.

Furthermore, Clients can login to the Website with the username and password which they receive from the Service provider when entering into the agreement, and they can perform administrative and other tasks in connection with the Service, according to their agreement, on the online management platform on the Website, moreover, they can have a look at information, dashboards, reports and statistics in connection with the Service provided. For this login, registration and an agreement with the Service provider is required.

The services on the Website and the Services are only available for persons who reached the age of 18 years. The services for which the Client's registration is required, shall only be used by the Clients for themselves, in case someone logs in to the website in the name of the Client, they guarantee that they are in possession of a proper authorization from the Client regarding the processing and forwarding of their data.

The Users and Clients are liable for the data provided by them and for the content uploaded by them, the Service provider shall not be held liable for those.

### **4. How does the present notice apply to the Users?**

By entering the Website, by using the services thereon, and by using any of the Website's functions, the Users automatically acknowledge the content of the present notice without any separate statements.

### **5. How and by whom may this notice be amended, and how and where is it published by Service Provider?**

The Service provider may unilaterally amend this notice at any time. The service provider publishes the amendment of the notice in a joint, amended version on the Website, under a separate menu item. We request the Users to carefully read the present notice at every Website visit.

The present notice is continuously available on the Website. The Users may open, view, print, save the notice, but may not amend them, only Service Provider may do so.

### **6. What personal data do we process, for how long, for what purposes and on the basis of what authorization?**

The legal bases for our data processing are the following:

- a) GDPR Article 6 (1) a) where the processing is based on the informed consent of the data subject (hereafter referred to as **Consent**)
- b) GDPR Article 6 (1) b), on where processing is necessary for the performance of a contract to which the data subject is party (hereafter referred to as **Performance of a Contract**)
- c) GDPR Article 6 (1) c) where data processing is necessary for the fulfilment of or compliance with a legal obligation of the data controller (e.g. obligations with tax statues – hereafter referred to as **Compliance**)
- d) GDPR Article 6 (1) f) where data processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, (hereafter referred to as **Lawful interest**)
- e) the data processing authorization afforded by Article 13/A of Act CVIII of 2001 on Electronic Commerce and on Information Society Services, where data controllers are authorized to process the natural identification data and home address of the recipients without the need for consent, as required for contracts for information society services, for defining their contents, for subsequent amendments and for monitoring performance of these contracts, for invoicing the relevant fees, and for enforcing the claims arising out of or in connection with such contracts., moreover, where data controllers are authorized to process natural identification data and home address for the purposes of invoicing for the fees payable under the contracts for the provision of information society services to the extent related to the use of information society services, and information relating to the date, the duration and the place of using the service (hereafter referred to as **E-Commerce**).

**6.1. Processing the contact information of Clients contacting the customer service or technical support**

<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>
<b>Category of the data subject</b>	<b>Category of data</b>	<b>Data source</b>	<b>Purpose of data processing</b>	<b>Legal basis of data processing</b>	<b>Storage period, deletion time</b>
Contact person of the Client turning to the customer service or technical support	Name	Given by data subject	Identification Investigating the complaint Administration Claim and law enforcement	GDPR Article 6 (1) f) Legitimate interest	5 years
	Phone number	Given by data subject	Identification Investigating the complaint Administration Claim and law enforcement	GDPR Article 6 (1) f) Legitimate interest	5 years
	E-mail address	Given by data subject	Identification Investigating the complaint Administration Claim and law enforcement	GDPR Article 6 (1) f) Legitimate interest	5 years
	Complaint, question, request submitted	Given by data subject	Identification Investigating the complaint Administration Claim and law enforcement	GDPR Article 6 (1) f) Legitimate interest	5 years

The customer service and technical support can be used by our Clients. Our Clients may contact the customer service through their contact persons and may ask for technical support from our personnel via e-mail or phone, regarding the Services used by them. When contacting the customer service, it is obligatory for the Client's contact person to provide their name, in the case of e-mail customer service, also their e-mail address, in the case of phone customer service, their phone number, for the sake of identification and further administration; without this, the Service provider is not able to receive or investigate the complaint, question or request and is not able to manage further administration. The scope of the data which is necessary for the sake of identification, investigating complaints, fulfilling requests, answering questions, providing technical support, managing further administration and for claim and law enforcement in connection with complaints, is narrow, and it is also in the legitimate interest of the Client and the Service Provider, which does not violate or does not pose a threat to the fundamental rights and freedoms of data subjects.

The period of processing and storing data in connection with the consultation with the customer service corresponds with the limitation period of 5 years prescribed by civil law; the storage of data is necessary within this limitation period for the sake of claim and law enforcement.

## 6.2. Regarding the login information of the Clients

<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>
<b>Category of the data subject</b>	<b>Category of data</b>	<b>Data source</b>	<b>Purpose of data processing</b>	<b>Legal basis of data processing</b>	<b>Storage period, deletion time</b>
Client	Username	Given by data subject	a) Client identification b) Access to the online management platform c) Performance of a Contract d) Claim and law enforcement	In case of processing purposes of D/a)- c): GDPR Article 6 (1) b) Performance of a contract In case of processing purposes of D/d: GDPR Article 6 (1) f) Legitimate interest	5 years from the termination of the contract
	Password	Given by data subject	a) Client identification b) Access to the online management platform c) Performance of a Contract d) Claim and law enforcement	In case of processing purposes of D/a)- c): GDPR Article 6 (1) b) Performance of a contract In case of processing purposes of D/d: GDPR Article 6 (1) f) Legitimate interest	5 years from the termination of the contract

Clients can login to the online management platform of the Website with the username and password which they receive from the Service provider when entering into the agreement. These data is stored by the Service provider within the limitation period of 5 years prescribed by civil law for the sake of the performance of the contract with the Clients, and in the case of claim and law enforcement for the sake of having evidence later on. Data processing for the sake of claim and law enforcement is also in the legitimate interest of the Service Provider and the Client, it makes it possible to prove that it was the Client itself who logged in to the online management platform. The scope of the data which is necessary for claim and law enforcement is narrow, and it is also in the legitimate interest of the Client and the Service Provider, which does not violate or does not pose a threat to the fundamental rights and freedoms of data subjects.

### 6.3. Regarding sending unsolicited proposals and marketing messages

A	B	C	D	E	F
Category of the data subject	Category of data	Data source	Purpose of data processing	Legal basis of data processing	Storage period, deletion time
Recipients of the proposals and marketing messages	name	Given by data subject	Electronic direct marketing messages, sending newsletters through direct marketing	GDPR Article 6 (1) a) Consent	Until the withdrawal of consent
	e-mail address	Given by data subject	Electronic direct marketing messages, sending newsletters through direct marketing	GDPR Article 6 (1) a) Consent	Until the withdrawal of consent

From time to time, the Service provider sends messages to the Clients via their contact persons, or potential clients which are not Clients of the Service provider yet, via e-mail, regarding proposals and news about the Service provider or services provided by the Service provider.

We only send proposals, marketing messages and electronic messages to recipients which have given their consent thereto. Consent may be given by sending an email to the [support@arenintel.com](mailto:support@arenintel.com) e-mail address or in any other way which can be proven later on. The consent to receiving proposals and marketing messages may be withdrawn by sending an email to the [support@arenintel.com](mailto:support@arenintel.com) e-mail address, or sending a mail to the address of the Service provider, or on the phone number of the Service provider's customer service; in case of withdrawal of consent, we will not send any more proposals or marketing messages.

After withdrawing consent, consent may be given again at any time. Consent is not a condition of using any of the Services. It is obligatory to provide e-mail address and name when giving consent. For withdrawing consent it is also obligatory to provide e-mail address and name, for the sake of identification.

### 6.4. Regarding System notifications

We send system notifications to our Clients by e-mail, via their contact persons, regarding the operation, technical accessibility, maintenance, the agreement concluded between them and the billing of the fees specified in the agreement (hereinafter referred to as: **System notification**). We process the following data in connection with system notifications:

A	B	C	D	E	F
Category of the data subject	Category of data	Data source	Purpose of data processing	Legal basis of data processing	Storage period, deletion time
Contact person of the Client	name	Client	a) Sending a system notification b) Claim and law enforcement	In case of processing purposes of D/a): GDPR Article 6 (1) b) Performance of a contract	5 years from the termination of the contract

				In case of processing purposes of D/b): GDPR Article 6 (1) f) Legitimate interest	
	e-mail address	Client	a) Sending a system notification b) Claim and law enforcement	In case of processing purposes of D/a): GDPR Article 6 (1) b) Performance of a contract  In case of processing purposes of D/b): GDPR Article 6 (1) f) Legitimate interest	5 years from the termination of the contract

Sending System notifications is in the legitimate interest of the both the Service provider and the Client, the Service provider can inform the Client about the availability, failure, maintenance and other feature of a Service in a System notification. The Service provider stores the System notifications sent to the Clients, within the limitation period of 5 years prescribed by civil law, for the sake of potential claim and law enforcement, settling debates and for the sake of having evidence later on. The scope of the data which is necessary for claim and law enforcement is narrow, and it is also in the legitimate interest of the Client and the Service Provider, which does not violate or does not pose a threat to the fundamental rights and freedoms of data subjects.

The period of processing and storing data in connection with the consultation with the customer service corresponds with the limitation period of 5 years prescribed by civil law; the storage of data is necessary within this limitation period for the sake of claim and law enforcement.

### 6.5. Processing data of the Clients' contact persons

The Service provider processes the data of the Clients' contact persons for the sake of the performance of the contract with the Client, and for the sake of communication with the Client, as per the following:

<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>
<b>Category of the data subject</b>	<b>Category of data</b>	<b>Data source</b>	<b>Purpose of data processing</b>	<b>Legal basis of data processing</b>	<b>Storage period, deletion time</b>
<b>Clients' contact persons</b>	name	Client	a) Communication b) Performance of the contract c) Claim and law enforcement	GDPR Article 6 (1) f) Legitimate interest	In case the data is included in the contract: 8 years from the termination of the contract In case the data is not included in the contract: 5 years from the termination of the contract

	phone number	Client	a) Communication b) Performance of the contract c) Claim and law enforcement	GDPR Article 6 (1) f) Legitimate interest	In case the data is included in the contract: 8 years from the termination of the contract In case the data is not included in the contract: 5 years from the termination of the contract
	e-mail address	Client	a) Communication b) Performance of the contract c) Claim and law enforcement	GDPR Article 6 (1) f) Legitimate interest	In case the data is included in the contract: 8 years from the termination of the contract In case the data is not included in the contract: 5 years from the termination of the contract
	position	Client	a) Communication b) Performance of the contract c) Claim and law enforcement	GDPR Article 6 (1) f) Legitimate interest	In case the data is included in the contract: 8 years from the termination of the contract In case the data is not included in the contract: 5 years from the termination of the contract

It is in the legitimate interest of both the Service provider and the Client that the Service provider is able to contact the Client at any time, via its contact persons. The scope of the contact persons' data is narrow, they only contain information which is necessary for sending notifications, the phone number and e-mail address usually serves business communication purposes, thus it does not affect the fundamental rights and freedoms of the contact person disproportionately.

In case the data is included in the contract, the storage period corresponds with the storage period prescribed by the Act on Accounting. In case the data is not included in the contract, the storage period corresponds with the general limitation period of 5 years prescribed by civil law.

#### **6.6. Data processing in connection with the request for offers**

Anyone can request an offer from the Service provider in connection with its services, either on the Website by filling out the form, or by sending an email to the Service provider.

The data processing of contact information is in the legitimate interest of both the data controller and the partner requesting an offer, since it is necessary for the data controller in order to send an offer to the partner, upon the request of the partner, and to maintain contact with the partner in connection with the offer. The data controller only processes the data of the contact person which is strictly necessary, thus the fundamental rights and freedoms of the contact person are not violated by the data processing, and they do not prevail over the above mentioned legitimate interests of the data controller and the partner requesting an offer.

The Service provider processes the following data in the case of a requested offer:

A	B	C	D	E	F
Category of the data subject	Category of data	Data source	Purpose of data processing	Legal basis of data processing	Storage period, deletion time
<b>Contact person of the person requesting an offer</b>	name	Data subject	Sending an offer, entering into an agreement	GDPR Article 6 (1) f Legitimate interest	5 years from sending the offer (limitation period)
	phone number	Data subject	Sending an offer, entering into an agreement	GDPR Article 6 (1) f Legitimate interest	5 years from sending the offer (limitation period)
	e-mail address	Data subject	Sending an offer, entering into an agreement	GDPR Article 6 (1) f Legitimate interest	5 years from sending the offer (limitation period)
	content of the message	Data subject	Sending an offer, entering into an agreement	GDPR Article 6 (1) f Legitimate interest	5 years from sending the offer (limitation period)

#### 6.7. Processing data collected automatically via the Website

We use cookies and other various programs on the Website in order to understand the Website visitors' preferences and behaviour relating to the Website, to develop the Webpage based on those, and to generate anonymous statistics on Website traffic. Certain small programs aid the Users in not having to enter their data again at the subsequent login, and to make their identification easier and quicker, while other programs serve to identify the Users. We elaborate on this data collection below:

Category of the data subject	Category of data	Data source	Purpose of data processing	Legal basis of data processing	Storage period, deletion time
<b>Users visiting the Website</b>	IP address, country, browser used, type and version number of the device and operating system, language settings, time of visit	Collected automatically by the Service provider	Generating statistics Developing the website Identification of the user	GDPR Article 6 (1) f Legitimate interest	2 years from the visit
	Website visiting information (pages visited, time spent on the Website, clicks, pages opened)	Collected automatically by the Service provider	Generating statistics Developing the website Identification of the user	GDPR Article 6 (1) f Legitimate interest	2 years from the visit

The above mentioned processing of data is in the legitimate business interest of the Service provider since it can ensure the development and safety of its website. The scope of the collected and processed data is narrow, these are merely used for anonymous statistics and analyses, it is not used to identify behaviours or preferences, and no automated decisions are made based thereon, no personalised offers are made by the Service provider based thereon. Therefore, the fundamental rights and freedoms of the Users are not affected disproportionately.



Upon visiting the Website and using the Services, we place cookies in User's browser and in HTML-based emails in accordance with the present data management notice.

In general, the cookie is a small file consisting of letters and numbers which is sent to the device of the User from the web server of the Service provider. It enables for the Service provider to recognize the last time when the User logged in to the Website. The main purpose of the cookie is to make it possible for the Service provider to provide individualized offers and advertisements for the User which personalizes the User's experience during the use of the Website and may reflect more to the personal needs of the User.

**Purpose of cookies used by the Service provider:**

- a) Security: aiding and ensuring safety, moreover enabling and aiding Service provider to detect unlawful conduct.
- b) Preferences, attributes and services: cookies let Service provider know, what language is preferred by the User, what are their communications preferences, aid the User in completing forms on the Website, making them easier to fill out.
- c) Performance, analytics and research: cookies aid the Service provider in understanding how the Website performs in various areas. The Service provider may use cookies, which rate, improve and search the Website, the products, functions, services, including when User enters the Website from other websites, and the devices, such as User's computer or mobile device.

**Types of cookies used by Service Provider:**

- a) analytics, tracking cookies;
- b) session cookies, which only operate during the active session (usually the webpage visit itself);
- c) permanent cookies: which help identifying the User as an existing User, making it easier for them to return to the Website without having to log in again. After the User logs in, the permanent cookie remains in their browser, with the webpage being able to read it when the User returns to the Website.

Adobe Flash is another technology which has the same function as cookies. Adobe Flash is able to store data on the User's device. However, not every browser allows the removal of Adobe Flash cookies. The User may restrict or block Adobe Flash cookies via the website of Adobe. If the User restricts or blocks them, certain elements of the Website may become unusable.

**Third party cookies:**

Reliable partners aid the Service provider in displaying advertisements on the Website and outside of the Website, and analytics companies such as Google Analytics, Quantcast, Nielsen and ComScore may also place cookies on the User's device.

Users may disallow Google cookies on the page used for the disabling Google ads. On <http://www.networkadvertising.org/choices/> there are further means to disable other third party cookies.

**Control of cookies:**

Most cookies enable Users to control cookie use via their settings. However, if the User restricts the usage of cookies, this may hinder user experience, since it will no longer be customised. Users may also stop the saving of personal settings, such as saving login information.

If the User does not wish the Service provider to use cookies when the User visits the webpage, Users may disable cookies directly in the cookie banner. In order to let the Service provider know that the User disabled the use of cookies, a denial cookie is placed on the User's device, thus Service provider will know that no cookies may be placed on that device at the next Website visit. If the User does not wish to receive cookies, they may change their browser settings accordingly. If no such change has been made, the Service provider will consider that the User has consented to the use of cookies. The Website does not function properly without cookies.

For further information of cookies, including types, management and removal, visit Wikipedia.org, [www.allaboutcookies.org](http://www.allaboutcookies.org) or [www.aboutcookies.org](http://www.aboutcookies.org).

## 7. Who manages your personal data, and who has access to them?

### 7.1. The data controller

The controller of the personal data specified under point 6 is the Service provider, the contact details and company data of which are the following:

#### **Arenim Technologies Fejlesztő és Szolgáltató Kft.**

Seat: 1095 Budapest, Lechner Ödön fasor 6.  
Head office: 1095 Budapest, Lechner Ödön fasor 6.  
Company registration number: 01-09-330669  
Tax number: 12904327-2-43  
Represented by: Attila Molnár Megyeri, Managing Director; contact details: at the seat of the company, in his office and by phone  
Phone number: +36-1-8555-111  
+36-1-4454-123  
E-mail address: info@arenim.com  
Website: [www.arenimtel.com](http://www.arenimtel.com), [www.arenim.com](http://www.arenim.com) and [www.webwithme.com](http://www.webwithme.com)

On the side of Service provider the data is accessible to the employees of the Service provider, whose access is essential in order to perform their duties. Access authorizations are specified in a strict internal code.

### 7.2. The data processors

For processing personal data, we engage the following companies, with whom we have entered into data processor agreements. The following data processors process personal data:

Name and address of the data processor	Purpose of data processing	Data processed
MiniCRM Zrt. (1075 Budapest, Madách Imre út 13-14.; Company registration number: 01-10-047449; Tax number: 23982273-2-42)	User database management, CRM system	Data mentioned in point 6.3., 6.4., 6.5. and 6.6.

Tresorit Kft. (1092 Budapest, Köztelek utca 6-8.; Company registration number: 01-09-969460; Tax number: 23520152-2-43)	Document management	Data mentioned in point 6.5., 6.6.
Hetzner Online GmbH (registration number: HRB 6089; Tax number: DE812871812; seat: Industriestrasse 25, 91710 Gunzenhausen)	Server lease, server hosting	Data mentioned in point 6.1 . – 6.7.
Servergarden Kft. (1023 Budapest, Lajos utca 28-32.; Company registration number : 01-09-186097; Tax number: 24855608-2-41)	Server lease, server hosting	Data mentioned in point 6.1 . – 6.7.
Magyar Telekom Nyrt. (1097 Budapest, Könyves Kálmán krt. 36.; Company registration number: 01-10-041928; Tax number: 10773381-2-44)	Server lease, server hosting	Data mentioned in point 6.1 . – 6.7.
Amazon.com Inc. (Amazon Web Services - 2021 Seventh Ave Seattle, Washington 98121)	Cloud services	Data mentioned in point 6.1 . – 6.7.
Microsoft Corporation (Microsoft 365 - One Microsoft Way Redmond, Washington 98052)	Cloud services	Data mentioned in point 6.1 . – 6.7.
SurveyMonkey Europe UC (2 Shelbourne Buildings, Second Floor, Shelbourne Rd, Ballsbridge, Dublin 4, Ireland)	Online survey services	Data mentioned in point 6.1 . – 6.7.
Google LLC. (USA)	Analytics services	Data mentioned in point 6.3., 6.7.
iWebMa Magyarország Kft. (1132 Budapest, Visegrádi u. 31.; Company registration number: 01-09-914318; Tax number: 14666641-2-41)	Analytics services	Data mentioned in point 6.3., 6.7.
SendGrid, Inc. (1801 California Street, Suite 500 Denver, Colorado 80202)	Newsletter sending services	Data mentioned in point 6.3., 6.4.

The U.S.-based data processors from the above list (Amazon.com, SendGrid, Inc., Microsoft Corporation and Google LLC) are part of the European Commission’s adequacy decision laid down in Article 45 of the GDPR and regulation no. 2016/1260 of the European Commission, and also on the U.S. – EU Privacy Shield List, thus data transfer to these companies shall not be considered as data transfer to third countries, outside of the EU, and the explicit consent of the data subjects is not required, furthermore transferring data to these companies is allowed under Article 45 of the GDPR. These companies undertook to comply with the GDPR.

**8. Who is the data protection officer of the Service provider and what are their contact details?**

The Service provider is not obliged to appoint a data protection officer.

**9. To whom do we forward your personal data?**

Your personal data is being forwarded exclusively to data processors mentioned in point 7.2., not to any other third party.

**10. What kind of rights do you have regarding the processing of your data, and how can you exercise them?**

- a) **Right of access:** you may inquire as to what data is managed, for what purposes, for how long, to whom do we forward them, and where the data originates from.
- b) **Right of correction:** should your data change or be recorded wrong, you may request that this be rectified or corrected. We would like to ask you to check your data regularly and to inform us about any change thereof within 15 days of the change, making it possible for us to keep our database up-to-date and correct.
- c) **Right of erasure:** in instances specified by law, you may request that we erase your stored personal data.
- d) **Right to restriction of processing:** in instances specified by law, you may request that data management be restricted regarding your personal data.
- e) **Right to object:** in case the data processing is based on legitimate interest, you may object to your personal data being managed, in which case we do not manage your personal data any further.
- f) **Right to data portability:** by filling out the request for data portability attached to the present notice, you may request us to hand over your personal data prescribed by law, either to you personally or upon a separate request and mandate to a service provider selected by you. We would like to draw your attention to the fact that the request for data portability may only be submitted with regard to data given by you, processed by us automatically and based on your consent, and that we are only able to fulfil a request for handing over data to another service provider, if it is technically possible and safe.

In cases of such requests, we will act according to the relevant and applicable law, and will provide you with information in one month regarding the measures taken by us.

- g) **Right to revoke consent:** in cases where personal data is processed based on the consent of the subject, they have the right to revoke such consent at any time, which does not affect the legality of data management conducted prior to the revocation.
- h) **Right to lodge a complaint:** should you have any complaints or grievances regarding our data management, you have the right to lodge a complaint by the supervisory authority:

National Authority for Data Protection and Freedom of Information

Website: <http://naih.hu>

Postal address: 1530 Budapest, Pf.: 5.

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

Phone number: +36 (1) 391-1400

Moreover, you may initiate a lawsuit against the Service provider if your right to personal data has been infringed.

The above mentioned rights may be exercised by sending an e-mail to [support@arenimtel.com](mailto:support@arenimtel.com) or by sending a mail to the seat of the data controller; in the event of this, we will act according to the relevant and applicable law, and will provide you with information in one month regarding the measures taken by us based on your request.

With regard to the right of access we would like to inform you that in case the data processed solely on a paper format and it also contains personal data of third persons, we are not in the position to provide you with a copy thereof based on Article 15 (3) and (4) of the GDPR, since in case the data is exposed to unauthorized persons, the rights of the third persons are violated.

In case the exercise of the right of access or a request thereto is clearly unfounded, or it is considered excessive due to its repetitive nature (a request shall be considered excessive when it is submitted more than 2 times per year, regarding the same scope of data), we charge an administration fee of 10 000,- HUF ( - namely - ten thousand forint ) + VAT for every further request for a copy.

## **11. How do we ensure the safety of your data?**

Service Provider has introduced and implemented the following information security procedures for the purposes of data protection:

We have a detailed information security code, business continuity code, document management code and incident management code regarding the safety of the data and information that we process, which is mandatory for all of our personnel, and which is known and practised by our staff.

We regularly coach and train our employees regarding data and information security requirements.

### **11.1. Data security in IT infrastructure**

We store personal data on a rented server, in a cloud and on the hard drives of company computers; the access thereto is strictly controlled and only granted to a very restricted circle of personnel.

The data and documents stored in the document management system are being stored encrypted, access is only possible with a password and proper authorization. The data in the internal IT network also run encrypted. Data on the company mobile phones are stored on encrypted storage sites. Our local computers are encrypted, unlocking the local hard drive is only possible with a password. Access usernames and passwords are being stored in password safes or in another secure way.

Our servers are located in professional server parks, in strictly guarded server rooms, which are water-, and fire-proof, and also protected against intrusion.

Our IT systems are tested and monitored repeatedly and regularly from time to time, in order to ensure and maintain data- and IT safety.

Office workstations are password-protected, third-party storage devices are restricted and may only be used following approval.

Regular and continuous protection against malicious software is provided regarding all of the systems and system elements of the Service Provider.

During the planning and operation of programs, applications and tools, we address security functions separately and with emphasis.

When allocating authorisations to our IT systems, we pay close attention to the protection of data (e.g. passwords, authorisations, logs) affecting the safety of these systems.

We generate backups daily and store them for 6 days; weekly backups are stored for 4 weeks. Our servers are redundant, and full backups are generated. The backups may only be accessed by a restricted circle of personnel.

#### **11.2. Data security in communication**

Regarding electronically forwarded messages and files, we secure the integrity of data on both the controller's and the user's side, in order to comply with the requirement of safe data exchange. In order to avoid data loss and damage, we use failure detecting and correcting processes. We use the protection functions of an endpoint-endpoint level of authorization control, ensuring accountability and auditability on the network.

Our implemented security measures detect unauthorized modifications, embedding and repetitive broadcasting. We prevent data loss and damage by fault detecting and correcting processes and we ensure the prevention of deniability.

Regarding the network used for data transmission, we provide appropriate measures to prevent illegal connection and eavesdropping per an adequate security level.

#### **11.3. Data security in document management**

We comply with data security requirements in document management as well, which we stipulated in our document management code. We manage documents by pre-set written access authorization levels, based on the level of confidentiality regarding the documents. We follow strict and detailed rules regarding the destruction of documents, their storage and handling at all times.

#### **11.4. Physical data security**

In order to provide physical data security, we ensure that our doors and windows can be properly closed and locked, and we keep strict access control regarding our visitors at all times.

We store paper documents containing personal data in a closed locker that is fire- and theft-proof, and to which only a limited circle of personnel has access.

The rooms where storage devices are placed have been designed to provide adequate protection against unauthorised access and breaking and entering, as well as fire and environmental damage. The storage of data transit, backups and archives is done in reliably closed locations.

**12. What procedure do we follow upon an incident?**

According to the relevant and applicable law, we report incidents to the supervisory authority within 72 hours of having become aware of it, and we also keep record of them. In cases regulated by the relevant and applicable law, we also inform the subjects of the incidents, and we act according to our incident management code.

**13. When and how do we amend this notice?**

Should the scope of data or other circumstances of data management be subject to change, this notice shall be amended and published on [www.arenimtel.com](http://www.arenimtel.com) and [www.arenim.com](http://www.arenim.com) within 30 days, as is required by the GDPR. Please always read the amendments of this notice carefully, as they contain important information regarding the management of your personal data.