DATA MANAGEMENT NOTICE
REGARDING THE MANAGEMENT OF DATA OF THE CLIENTS' CONTACT PERSONS

Enters into force: February 14, 2024

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: **Controller**) hereby informs its Clients about the processing of data of the Clients' contact persons, 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**).

The present data management notice is annexed to and constitutes an inseparable part of the agreement concluded between the Controller and the Client.

The present data management notice shall be handed over to the contact persons of the Client and the Client shall provide proof to the Controller of having done so.

1. What personal data of the contact persons do we process, for how long, for what purposes and on the basis of what authorization?

The legal basis for our data processing is the following:

a) 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.

Processing the data of the contact persons is in the common legitimate interest of the Controller and the Client, since it is necessary for the performance of the agreement concluded between the Controller and the Client, for communication regarding the agreement, and for sending notifications to the Client in connection with the agreement. 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 legitimate interests of the data processor and the Client.

The legal basis of data processing is specified below by category and by purpose of data processing.

A	B	C	D	E
Category of data	**Data source**	**Purpose of data processing**	**Legal basis of data processing**	**Storage period, deletion time**
name	Client	Communication Performance of the contract 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			
e-mail address	Client			
position	Client			

2. Who manages the personal data of the contact persons, and who has access to them?

2.1. The data controller

The controller of the personal data mentioned in point 1 is **Arenim Technologies Fejlesztő és Szolgáltató Kft.,** the contact details and company data of which are the following:

Seat and head ofice:	1095 Budapest, Lechenr Ödön fasor 6.
Company registration number:	01-09-330669
Tax number:	12904327-2-43
Represented by:	János Angyal Managing Director; contact details: at the seat of the company, in his office and by phone
Phone number:	+36-1-8555-111 or +36-1-4454-123
E-mail address:	info@arenimtel.com
Website:	www.arenimtel.com, www.arenim.com and www.webwithme.com

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

2.2. Data processors

For processing and storing personal data of the contact persons, 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 1.
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 1.
Hetzner Online GmbH (registration number: HRB 6089; Tax number: DE812871812; seat: Industriestrasse 25, 91710 Gunzenhausen)	Server lease, server hosting	Data mentioned in point 1.
Servergarden Kft. (1139 Budapest, Váci út 99-105. Balance Building. ép. 3. em.; Company registration number: 01-09-350297; Tax number: 27116328-2-41)	Server lease, server hosting	Data mentioned in point 1.

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 1.
Invitech ICT Services Kft. (1013 Budapest, Krisztina körút 39.; Company registration number: 01-09-414291; Tax number: 25836965-2-44)	Server lease, server hosting	Data mentioned in point 1.
Amazon Web Services EMEA SARL (38 Avenue John F Kennedy, L-1855 Luxembourg; Company registration number: 10048410; Tax number: LU26888617)	Cloud services	Data mentioned in point 1.
Microsoft Ireland Operations Ltd, (One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521 Ireland, Adószám: IE8256796U)	Cloud services	Data mentioned in point 1.
Google Ireland Limited (Gordon House, Barrow Street, Dublin 4, Ireland, Tax number: IE6388047V)	Analytics services	Data mentioned in point 1.
iWebMa Magyarország Kft. (1061 Budapest, Király utca 26.; Company registration number: 01-09-914318; Tax number: 14666641-2-42)	Analytics services	Data mentioned in point 1.
Horizont Informatika Kft. (4034 Debrecen, Repce u. 3.; Company registration number: 09-09-010685; Tax number: 13282895-2-09)	Website maintenance, analytics services	Data mentioned in point 1.
Twillio SendGrid Inc. (101 Spear Street, Ste 500 San Francisco, CA 94105 Tax number: 26-2574840)	Newsletter sending services	Data mentioned in point 1.

3. Who is the data protection officer of the Controller and what are their contact details?

The Service provider is not obliged to appoint a data protection officer according to the relevant provisions of the GDPR.

4. To whom do we forward your personal data?

The personal data of the contact persons is being forwarded exclusively to data processors mentioned in point 2.2., not to any third country not being a contracting state to the GDPR.

5. What kind of rights do the contact persons have regarding the processing of their data, and how can they exercise them?

a) Right of access: they 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.

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 for every further request for a copy.

b) Right of correction: should their data change or be recorded wrong, the contact persons may request that this be rectified or corrected.

c) Right of erasure: in instances specified by law, they may request that we erase their stored personal data.

d) Right to restriction of processing: in instances specified by law, they may request that data management be restricted regarding their personal data.

e) Right to object: in case the data processing is based on legitimate interest, they may object to their personal data being managed, in which case we do not manage their personal data any further.

f) Right to data portability: they may request us to hand over their personal data prescribed by law, either to them personally or upon a separate request and mandate to a service provider selected by them, in case it is technically possible and safe.

The above mentioned rights may be exercised by sending an e-mail to 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.

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.

Consent may be withdrawn electronically, by sending an e-mail to our e-mail address (support@arenimtel.com) or by sending a mail to the seat of the data controller

h) **Right to lodge a complaint:** should the contact persons have any complaints or grievances regarding our data management, they 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
Phone number: +36 (1) 391-1400

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

6. How do we ensure the safety of your data?

6.1. 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 to those company computers 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 data controller.

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

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

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

6.2. 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.

6.3. 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.

6.4. 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 unauthorized access and breaking and entering, as well as fire and environmental damage. Data transit, as well as the storage of backups and archives is done in these reliably closed locations.

7. 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.

8. 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 and 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.