IMIMEMO.CH

IMI MEMO

General Terms and Conditions

Introduction

The Terms and Conditions Agreement of IMIMEMO (hereinafter: the Agreement) contains the conditions and rules for the use of the services available on the website / application (https://imimemo.ch/, hereinafter: Imimemo) operated by IMIMEMO (hereinafter: Service Provider).

Service provider information

Contact details of the service provider, regularly used e-mail address for contacting users: hello@imimemo.ch

Scope and fundamentals:

1. Issues not regulated by this Agreement and the interpretation of this Agreement are both governed by and are to be construed in accordance with Hungarian Law, in particular Act V of 2013 on the Civil Code and Act CVIII of 2001 on Electronic Commerce and on Information Society Services Government. Moreover, the relevant provisions of the Decree 45/2014. (II.26.) on Detailed Rules governing contract concluded between consumers and businesses are also applicable. The mandatory provisions of the relevant legislation shall apply to the parties without any specific stipulation.
2. This Agreement is effective from July 8, 2020 and will remain in force until revoked. The Service Provider is entitled to unilaterally amend the Agreement. The circumstances giving rise to the amendment are the following: change in legislation, business interest, changes within the company. In case of an amendment like this, the User has the right to withdraw from or terminate the contract. The amendments do not affect previously concluded contracts, as a result the amendment has no retroactive effect.
3. The Service Provider reserves all rights with regard to the website / mobile application, any part thereof and the content appearing on it, as well as the distribution of the website / mobile application. It is strictly prohibited to download, electronically store, process and sell the contents or any part of the content appearing on the website without the written consent of the Service Provider.

General provisions

1. Upon starting to use the Service, an online contract is concluded between the User and the Service Provider, under the conditions set forth in this Agreement.
2. The Service Provider reserves the right to modify or remove any content elements of the website / mobile application at any time without prior notice or to change their appearance, content and operation.
3. The Service Provider reserves the right to modify the content of the website / mobile application at any time or to terminate its accessibility in compliance with the provisions of these GTC.

Liabilities

1. The Service Provider undertakes 99.5% annual availability of its Web Services (mobile application and website). Parties exclude the Service Provider's liability for downtime and other anomalies beyond this error limit. Exceptions to this obligation are supplying accessibility and other operational tasks provided by another service provider.
2. The Service Provider shall not be liable if an external attack (e.g. hacker attack) affects the application provided by the Service Provider and as a result data loss or service interruption occurs. In such cases, the Service Provider shall repair the damages caused by the breach of the information system as soon as possible and restore the service.
3. The Service Provider shall not be liable for any malfunctions or access errors not attributable to the Service Provider or performed with the assistance of another Service Provider.
4. The Service Provider shall not be liable for the unavailability or slow operation of the system due to the fault of the Internet Service Provider.
5. The Service Provider's liability is excluded in case of all conduct (especially damage and loss) arising from the unprofessional, illegal, anti-GTC use of the mobile application - service, or in case the financial profit expected by the User by using the service is lower than expected, the lack of financial benefit or loss.
6. Service Provider shall also not be liable for any damages or losses of any kind resulting from the loss of personal or confidential information, the unusability of all or part of the hardware or software, personal injury, or failure to perform any obligation (including obligations arising out of negligence, good faith or reasonable judgment).
7. Providing the required internet access and the necessary devices (hardware and software and their appropriate settings) to use the service, is the User's responsibility.

Service fees

The Service is provided free of charge.

Conclusion of the contract

After requesting the trial version, the User can subscribe to the service in a separate contract. The service can be used within 1 week after concluding the contract.

Confidentiality

1. The Service Provider undertakes to protect, preserve and treat as confidential information the data, confidential data, information, confidential information and documents obtained during the performance of the service, and will make every effort to ensure their proper protection.
2. The Service Provider and the User may use the confidential data and information only for the purpose of performing the service, and may disclose the data and information to their knowledge only with the prior written consent of the other party, unless the disclosure is required by law.
3. The Service Provider undertakes that all data and information gained on the basis of these GTC shall be considered business secrets and as such, shall not be disclosed to third parties or used contrary to the purpose specified in the GTC.
4. The above obligation of confidentiality shall remain in force indefinitely for the duration of the service and after its termination for any reason as well.
5. The User is fully responsible for the use of all services which are accessible via his/her password. The User is fully responsible for keeping his/her password as a secret.
6. The Service Provider treats the personal data provided by the User within the framework of voluntary data provision confidentially, uses them only to the extent necessary for the identification of individual Users and the performance of the service. Moreover, the Service Provider uses the gained data to the extent necessary for successful performance and in accordance with §13/A of the Act CVIII of 2001 on Electronic Commerce and on Information Society Services Government.

Copyrights

1. Since all material contained on the website of https://imimemo.ch/ is protected by copyright laws, it is strictly prohibited to copy, distribute, transmit, display, perform, download (reproduce), publish, license, modify, rewrite, create derivative works from, transfer, or sell any material contained on the website without the prior written consent of the copyright owner.

2. In case of using any material from the website or database of https://imimemo.ch/ with

the prior written consent of the copyright owner, references to the website are still required. The Service Provider reserves all rights to all elements of its service, its domain names, the secondary domain names formed with them and its online advertisement spaces.

3. Adaptation or decryption of the content or parts of the website of https://imimemo.ch/ is strictly prohibited; along with unfair establishment of user IDs and passwords and usage of any application that modifies or indexes the website of https://imimemo.ch/ or any part thereof.

4. The name https://imimemo.ch/ is protected by copyright, its usage, except for the references, is possible only with the written consent of the Service Provider.

5. The User acknowledges that in case of unauthorized usage, the Service Provider is entitled to a penalty. The amount of the penalty is HUF 60,000 gross per image and HUF 20,000 gross per word. The user acknowledges that this penalty is not excessive and browses the site with this in mind. In the event of a copyright infringement, the Service Provider uses a notarized fact certificate, the amount of which is also due to the infringing user.

Right of termination

Based on Directive 2011/83 / EU of the European Parliament and the Council and Government Decree 45/2014 (II.26.) 29.§ (1) paragraph a.) and m.) points on the detailed rules for consumerbusiness
contracts. of the Government of the Republic of Hungary, the User is not entitled to the right of termination.

Data protection

The data management guidelines of the website are available at the following website: https://imimemo.ch//data_safety

Other provisions

1. The Service Provider is entitled to use a contributor to fulfill its obligations. The Service Provider is fully responsible for the contributor's unlawful conduct, as if the Service Provider had committed the unlawful conduct itself.

2. If any part of these Agreement becomes invalid, unlawful or unenforceable, it shall not affect the validity, legality and enforceability of the remaining parts.

3. If the Service Provider does not exercise some of its rights under this Agreement, the failure to exercise the given right shall not be considered a waiver of the given right. Waiver of any

right is only valid if expressly stated in writing by the Service Provider. If the Service Provider does not strictly adhere to some of the essential conditions or stipulations of the Agreement once, does not mean that it waives its strict adherence to the given condition or stipulation at a later date.

4. Both the Service Provider and the User shall endeavour to settle their disputes amicably.

5. The parties state that the Service Provider's website / mobile application operates in Hungary, and it is also maintained in Hungary. As the site can also be visited from other countries, the users expressly acknowledge that the applicable law in relation to the User and the Service Provider is the Hungarian law. If the user is a consumer, then based on Section 26, paragraph 1 of the Code of Civil Procedure, the court of the defendant's (consumer's) domicile shall have exclusive jurisdiction over the consumer in disputes arising from this contract.

6. The Service Provider does not apply different general access conditions for access to the services on its website for reasons related to the User's citizenship, residence or place of establishment.

7. The Service Provider shall not apply different conditions to the payment transaction for the reasons related to the User's citizenship, residence or place of establishment, place of payment account, place of establishment of the payment service provider or place of issue of the cash substitute payment instrument within the Union.

8. The service provider shall comply with the measures against unjustified territorial content restrictions and other forms of discrimination based on the nationality, place of residence or place of establishment of the buyer within the internal market, as well as Regulations (EC) No 2006/2004 and (EU) 2017/2394 and 2009/22. / EC REGULATION (EU) 2018/302 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.

IMIMEMO
PRIVACY NOTICE AND INFORMATION ON THE PROCESSING OF PERSONAL DATA

IMI MEMO

Privacy policy

Introduction

The Imi Memo (hereinafter: Service Provider, data controller) submits itself to the following regulations:
On the protection of individuals regarding the processing of personal data and on the free movement of such data and repealing Regulation (EC) No 95/46 (General Data Protection Regulation) we provide the following information based on REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016).
This Privacy Policy governs the privacy of the following page (s) / mobile applications:
https://imimemo.ch/
The privacy policy is available at https://imimemo.ch//data_safety
Amendments to the Regulations shall enter into force upon publication at the above address.

Data controller and its contact details

Name: Work Mit Uns Kft.
Headquarters: 2750 Nagykőrös, Csillag utca 6
E-mail: info@workmituns.ch
Phone: +36306982603

Concept definitions

1. "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); that natural person is identifiable who, directly or indirectly, in particular by an identifier such as name, number, location, online identifier or one or more factors relating to the natural person's physical, physiological, genetic, mental, economic, cultural or social identity is identifiable;

2. "data management" means any operation or set of operations on personal data or data files, whether automated or non-automated, such as collection, recording, systematisation, segmentation, storage, transformation or alteration, retrieval, consultation, usage, communication, transmission, distribution or otherwise; by making available, harmonizing or linking, restricting, deleting or destroying;

3. " data controller" means the natural or legal person, public authority, agency or any 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 the processing are determined by Union or Member State law, the controller or the specific criteria for the designation of the controller may also be determined by Union or Member State law;

4. "data processor" means any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller;

5. "recipient" means any natural or legal person, public authority, agency or any other body to whom personal data are communicated, whether a third party or not. Public authorities that may have access to personal data in the context of an individual investigation in accordance with Union or Member State law shall not be considered as recipients; the processing of such data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of the processing;

6. "consent of the data subject" means a voluntary, specific and well-informed and unambiguous statement of the data subject's consent to indicate his or her consent to the processing of personal data concerning him or her, by means of a statement or an unequivocal statement of

confirmation;

7. "data protection incident" means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data which have been transmitted, stored or otherwise handled.

Principles for the processing of personal data

Personal data:
1. must be processed lawfully and fairly and in a way that is transparent to the data subject ("lawfulness, fair play and transparency");

2. must be collected only for specified, explicit and legitimate purposes and not be treated in a way incompatible with those purposes; further processing for data purposes for archiving in the public interest, for scientific and historical research purposes or for statistical purposes ("purpose limitation") shall not be considered incompatible with the original purpose in accordance with Article 89 (1);

3. they must be appropriate, relevant and limited to what is necessary for the purposes of the processing ("data saving");

4. must be accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data which are inaccurate for the purposes of the processing are erased or rectified without delay ("accuracy");

5. must be stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for a longer period only if the processing of personal data is carried out in accordance with Article 89 (1) for archiving in the public interest, for scientific and historical research purposes or for statistical purposes, in accordance with this Regulation; subject to the implementation of appropriate technical and organizational measures to protect its freedoms ("limited storage capacity");

6. processing must be carried out in such a way as to ensure adequate security of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage to personal data ("integrity and confidentiality"), using appropriate technical or organizational measures.

The data controller is responsible for compliance with the above and must be able to demonstrate such compliance ("accountability").

The data controller declares that its data processing is carried out in accordance with the principles set out in this section.

Request a trial

1. Fact of data collection, scope of data processed and **purpose of data management**:

Personal data	**Purpose of data management**	**Legal basis**
Name (contact person)	Identification	Article 6, paragraph 1), point b)
E-mail address (contact person)	Contacting, sending reply messages	Article 6, paragraph 1), point b)

Telephone number (contact person)	Keeping in touch	Article 6, paragraph 1), point b)
Message content	Required for a response	Article 6, paragraph 1), point b)
Date and time of contact / request	Performing a technical operation	Article 6, paragraph 1), point b)
The IP address at the time of contact / request	Performing a technical operation	Article 6, paragraph 1), point b)

The email address does not need to contain any personal information.

2. Stakeholders: All stakeholders who request a trial via the contact form.

3. Duration of data processing, deadline for erasure of data: If one of the conditions set out in Article 17 (1) of the GDPR is met, it lasts until the data subject's request for erasure.

4. The identity of the potential data controllers entitled to access the data, the recipients of the personal data: The personal data may be processed by the authorized employees of the data controller.

5. Description of the data subjects' rights in relation to data processing:

• The data subject may request from the controller access to, rectification, erasure or restriction of the processing of personal data concerning him or her, and

• the data subject has the right to data portability and the right to withdraw consent at any time.

6. The data subject may initiate access to the erasure, modification or restriction of the processing of personal data and the portability of the data in the following ways:

• via post at the address 2750, Nagykőrös, Csillag utca 6.

• via e-mail to info@workmituns.ch,

• via phone on +36306982603.

7. Legal basis for data processing: data subject's consent, Article 6, paragraph 1, point b.

8. Please be informed that

• this data management is necessary for making an offer or for taking pre-contractual steps.

• it is required to provide personal information so that you can contact us and request a trial version.

• failure to provide data has the consequence that you cannot contact the Service Provider, thus you cannot request a trial version.

Apply Google Analytics

1. This website uses Google Analytics, a web analytics service provided by Google, Inc. (“Google”). Google Analytics uses so-called "cookies", which are text files placed on your computer, to help the website analyse how users use the site.
2. The information created by the cookie about the website used by the user will normally be stored and stored on a Google server in the USA. By activating IP anonymization on the Website, Google will abbreviate the User's IP address within the Member States of the European Union or in other States party to the Agreement on the European Economic Area.
3. The full IP address will be transmitted to and truncated to Google's server in the United States only in exceptional cases. On behalf of the operator of this website, Google will use this information to evaluate how the user has used the website, to provide the website operator with reports on website activity and to provide additional services related to website and internet usage.
4. Within the framework of Google Analytics, the IP address transmitted by the User's browser is not reconciled with other data of Google. The User may prevent the storage of cookies by appropriate settings in the browser, however, please note that in this case, not all functions of this website may be fully available. Users may also prevent Google from collecting and processing information about their use of the Website (including their IP address) by cookies by downloading and installing the browser plugin available at the following link.
https://tools.google.com/dlpage/gaoptout?hl=hu

Handing cookies

1. The so-called ‘password-protected session cookies’, ‘shopping cart cookies’, ‘security cookies’, ‘required cookies’, ‘functional cookies’, and ‘cookies responsible for managing website statistics’ does not require prior consent from the users.
2. The fact of data management, the scope of managed data, unique identification number, dates, times.
3. Stakeholders: All stakeholders who visit the website.
4. The purpose of data management: To identify users and track visitors.
5. Duration of data management, deadline for erasure of data:

Type of cookie	**Legal basis of data management**	**Duration of data management**
Session cookies	In accordance with the CVIII Act of 2001 on certain aspects of electronic commerce services and information	Until the relevant visitor session is closed

	society services, Law 13 / A. § (3)	
Permanent or saved cookies	In accordance with the CVIII Act of 2001 on certain aspects of electronic commerce services and information society services, Law 13 / A. § (3)	Until they are deleted by the data subject
Statistics, marketing cookies	In accordance with the CVIII Act of 2001 on certain aspects of electronic commerce services and information society services, Law 13 / A. § (3)	1 month- 2 years

6. Identification of potential data controllers entitled to access the data: The data controller does not process personal data by using cookies.

7. Providing information about the rights of the data subjects related to data management: The data subject has the possibility to delete cookies in the Tools / Settings menu of browsers, usually under the settings of the menu item, Privacy.

8. Legal basis of data management: The data subject's consent is not required if the sole purpose of the use of cookies is the transmission of communications via an electronic communications network or the provision of an information society service specifically requested by the subscriber or user.

9. Most browsers allow your users to set which cookies they wish to save and allow (specific) cookies to be deleted again. If you restrict the storage of cookies on certain websites or do not allow third-party cookies, this may, in certain circumstances, result in our website no longer being used in its entirety. Here is information on how to customize cookie settings for standard browsers:

Google Chrome (https://support.google.com/chrome/answer/95647?hl=hu)

Internet Explorer (https://support.microsoft.com/hu-hu/help/17442/windows-internet-explorerdelete-manage-cookies)

Firefox (https://support.mozilla.org)

Safari (https://support.apple.com/guide/safari/sfri11471/mac)

The data processors used

Hosting provider

1. Activity performed by data processor: Hosting service
2. Name and contact details of the data processor:
   Imi memo has owns and operates its own servers.
3. Fact of data processing, scope of data processed: All personal data provided by the data subject.
4. Stakeholders: All stakeholders using the website / mobile application.
5. The purpose of data management: To make the website / mobile application available and to operate it properly.
6. Duration of data processing, deadline for erasing the data: The data processing lasts until the termination of the agreement between the data controller and the hosting provider or until the data subject's request for erasure to the hosting provider.
7. Legal basis for data processing: Article 6, paragraph 1), points c) and f) and the CVIII Act of 2001 on certain aspects of electronic commerce services and information society services, Law 13 / A. § (3). There is a legitimate interest in the proper operation of the website, protection against attacks and fraud.

Other data processors (if any)

Social media

1. The fact of data collection, the scope of the managed data: the registered name and the user's public profile picture on social media sites like Facebook / Twitter / Pinterest / YouTube / Instagram, etc.
2. Stakeholders: All stakeholders who have registered on Facebook / Twitter / Pinterest / YouTube / Instagram, etc. social media sites and “liked” the Service Provider's social site or contacted the data controller via the social site.
3. The purpose of data collection: To share, “like”, follow, and promote certain content elements, products, promotions or the website itself on social media sites.
4. Duration of data processing, deadline for the erasure of data, identity of potential data controllers entitled to access the data and description of data subjects' rights related to data processing: The data subject can gain information about the source of the data, its processing, management and legal basis on the given social media sites. Data management is carried out on these social media sites, so the duration and methods of data management, as well as the possibilities of deleting and modifying data are regulated by the given social media site.
5. Legal basis for data processing: the data subject's voluntary consent to the processing of his or her personal data on social media sites.

Rights of data subjects

1. Right of access

You have the right to receive feedback from the data controller as to whether your personal data is being processed and, if such processing is in progress, you have the right to access your personal data and the information listed in the Regulation.

2. Right to rectification

You have the right, to request the data controller, to correct inaccurate personal data concerning you without undue delay. Considering the purpose of the data processing, you have the right to request that the incomplete personal data be supplemented, among others, by means of a supplementary statement.

3. Right of erasure

You have the right to request the data controller, to erase any personal data concerning you without undue delay, and the data controller is obliged to delete personal data concerning you without undue delay under certain conditions.

4. The right of oblivion

If the controller has disclosed personal data and is obliged to erase it, it shall take reasonable steps,
including technical measures, considering the available technology and the cost of implementation, to inform the controllers that you have requested the erasure of the links leading to your personal data in question or copies or duplicates of such personal data.

5. Right to restrict data processing

You have the right to request the controller to restrict the processing of data if one of the following conditions is met:
• You dispute the accuracy of personal data, in which case the restriction applies to the period of time that allows the data controller to verify the accuracy of the personal data;
• the data processing is illegal and you oppose the erasure of the data and instead ask for a restriction on its use;
• the data controller no longer needs the personal data for the purpose of data processing, but you request them in order to make, enforce or protect legal claims;
• You objected to the data processing; in this case, the restriction applies for as long as it is established whether the legitimate reasons of the controller take precedence over your legitimate reasons.

6. The right to data portability

You have the right to receive the personal data about you, provided by you to a data controller, in

a structured, widely used, machine-readable format, and you have the right to transfer this data to another data controller without being hindered by the data controller to whom you have provided your personal data (...)

7. Right to protest

In the case of data processing based on a legitimate interest or public authority as a legal basis, you have the right to object at any time to the processing of your personal data (...), including profiling based on those provisions, based on reasons related to your own situation.

8. Protest against direct business acquisition

If your personal data is processed for the purpose of direct business acquisition, you have the right to object at any time to the processing of personal data concerning you for this purpose, including profiling, insofar as it relates to direct business acquisition. If you object to the processing of personal data for the purpose of direct business acquisition, the personal data may no longer be processed for this purpose.

9. Automated decision making in individual cases, including profiling

You have the right not to be covered by a decision based solely on automated data processing, including profiling, which would have legal effect on you or affect you to a similar extent.

The preceding paragraph shall not apply if the decision:

- is necessary for the conclusion or performance of a contract between you and the data controller;
- is governed by EU or Member State law applicable to the controller, which also lays down appropriate measures to protect your rights and freedoms and legitimate interests; obsession
- it is based on your explicit consent.

Deadline for action

The controller shall, without undue delay, but in any case **within 1 month** of receipt of the request, inform you of the action taken on the above requests.
If necessary, it can be **extended by 2 months**. The data controller shall inform you of the extension of the deadline, indicating the reasons for the delay, **within 1 month** from the receipt of the request.
If the controller does not take action on your request, it will inform you **without delay, but no later than one month after receipt of the request, of the reasons for the non-action** and of the fact that you can lodge a complaint with a supervisory authority and have a judicial remedy.

The security of data management

The data controller and the data processor shall implement appropriate technical and organisational measures, taking into account the state of scientific and technological knowledge and the cost of implementation, the nature, scope, context and purposes of the processing and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons, in order to ensure a level of data protection appropriate to the level of risk, including, where appropriate:

1. the pseudonymisation and encryption of personal data;
2. ensuring the continued confidentiality, integrity, availability and resilience of the systems and services used to manage personal data;
3. in case of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner;
4. a procedure for the regular testing, evaluation and assessment of the effectiveness of the technical and organisational measures taken to ensure the security of data management.
5. The data processed must be stored in such a way that unauthorised persons cannot have access to them. In the case of paper-based data carriers, by establishing physical storage and archiving procedures, and in the case of data managed electronically, by using a centralised access management system.
6. The method of storing the data by IT means shall be chosen in such a way that their deletion can be carried out at the end of the erasure period, taking into account the possibility of different erasure deadlines, or if otherwise necessary. Erasure shall be irreversible.
7. Paper data media shall be destroyed by shredding or by outsourcing to an external organisation, specialised in shredding. In case of electronic data carriers, physical destruction and, where necessary, prior secure and irretrievable deletion of the data shall be ensured in accordance with the rules on the disposal of electronic data carriers.
8. The data controller shall take the following specific data security measures:

In order to ensure the security of personal data managed on a paper basis, the Service Provider applies the following measures *(physical protection)*:

9. storing documents in a secure, properly lockable, dry room.
10. If personal data managed on paper basis need to be digitised, the rules applicable to digitally managed data shall apply.
11. The employee of the Service Provider performing data management may leave the premises where data management is taking place only by securing the data carriers entrusted to him or by closing the given premises.
12. Personal data may be accessed only by authorised persons and not by third parties.

13. The Service Provider's building and premises are equipped with fire and property protection equipment.

IT security

14. Computers and mobile devices (other data carriers) used during data management are in possession of the Service Provider.
15. The computer systems containing personal data used by the Service Provider are protected against viruses.
16. To ensure the security of the digitally stored data, the Service Provider uses data backups and archiving.
17. Access to the central server machine is only allowed to authorised and designated persons.
18. Access to data stored on the computers is only granted with a username and password.

Informing the data subject about personal data breach

If the personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons, the data controller shall inform the data subject without undue delay.
The information given to the data subject shall clearly and prominently describe the nature of the personal data breach and provide the name and contact details of the data protection officer or other contact person who can provide further information; describe the likely consequences of the personal data breach; describe the measures taken or planned by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

The data subject need not be informed if any of the following conditions are met:

- the data controller has implemented appropriate technical and organisational protection measures and these measures have been applied to the data affected by the personal data breach, in particular those measures, such as the use of encryption, which make the data non-interpretable to persons not authorised to access the personal data;

- the data controller has taken additional measures following the personal data breach to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;

- the provision of information would require a disproportionate effort. In such cases, the data subjects shall be informed by means of publicly disclosed information or by means of a

similar measure ensuring that the data subjects are informed in an equally effective manner.

If the data controller has not yet notified the data subject of the personal data breach, the supervisory authority may, after having considered whether the personal data breach is likely to present a high risk, order the data subject to be informed.

Reporting a data breach to the authority

The controller shall notify a personal data breach to the competent supervisory authority according to Article 55 without undue delay and, if possible, no later than 72 hours after the personal data breach has come to its attention, unless the personal data breach is unlikely to present risk to the rights and freedom of natural persons. If the notification is not made within 72 hours, it shall be accompanied by the reasons justifying the delay.

Review in case of mandatory data management

Unless the duration of the mandatory data management or the periodic review of its necessity is determined by law, local government regulation or a binding legal act of the European Union, the controller shall review, at least every three years from the start of the data management, whether the management of personal data processed by the controller or by a processor acting on its behalf or under its instructions is necessary for the purposes of the data management.

The controller shall document the circumstances and the results of this review, keep this documentation for ten years after the review and make it available to the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as the Authority) upon request.

Concluding comments

The following legislation has been taken into account in the preparation of this General Terms and Conditions:

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation) (GDPR) (27 April 2016);
- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: Info. Act);

- Act CVIII of 2001 - on certain aspects of electronic commerce services and information society services (in particular § 13/A);
- Act XLVII of 2008 - on the Prohibition of Unfair Commercial Practices against Consumers;
- Act XLVIII of 2008 - on the basic conditions and certain restrictions of economic advertising (in particular § 6);
- Act XC of 2005 on Freedom of Electronic Information;
- Act C of 2003 on electronic communications (specifically § 155);
- Opinion No 16/2011 on the EASA/IAB Recommendation on best practice in behavioural online advertising;
- Recommendation of the Hungarian National Authority for Data Protection and Freedom of Information on data protection requirements for prior information.