PRIVACY STATEMENT

SUMMARY

Personal, private information can only be collected and handled according to the laws and regulations.

DM messages will only be sent if there is special authorization allowing them. System messages can be sent without such requirements.

We store data with maximum available security.

We only allow third parties to access data if they have special permission to do so.

We provide information about the stored data to anyone and the deletion of the data can be requested by contacting us through the support *support@ivm.hu*email address.

INTRODUCTION

IVM Zártkörűen Működő Részvénytársaság -Privately Limited Company-, (102, Berényi street, Székesfehérvár, 8000, companies' register c: 07 10 001386, tax number: 23003097-2-07) (hereinafter: Service provider, data handler) accepts the responsibilities detailed in this guide.
The data protection registration number of the webpage: NAIH-84357/2015.

The data protection registration number of the newsletter: NAIH-84358/2015.

Act CXII, 20. § (1) of 2011 on Informational Self-determination and Freedom of Information, states that those concerned (in this case a webpage user, hereinafter: User) should be informed prior to the management of his data, if the data management is compulsory or **requires his consent.**
Prior the management of his data, the user must be notified comprehensibly and in detail about all facts concearning the management of his data, including its **purpose and claim, the person responsible for the handling and processing,** and the time period of the **data management.**
The user must be notified according to Info tv. 6. § (1), that his private information can be managed if consent is impossible to obtain or would require undue cost or effort, and the handling of the data

- is required for the fulfillment of legal liability, or

- is required for the fulfillment of legal liabilities of the data manager or a third person and this interest is proportional enough to limit the protection of private information.

In case the personal notification is impossible or require undue cost or effort, (as in case of a webpage), the notification can be done through making the following information public:

1. the fact that data collection is taking place
2. defining the circle of those affected
3. the purpose of the data collection
4. the time period of data collection
5. all individuals who can possible have the right to view and manage the data
6. the user's rights concerning data management and his options of legal remedies
7. if the data collection is being officially included into a data privacy record, its place and the public account number.

This Privacy Information Guide regulates the data management of the following websites: http://medical-vending.com and is based on the information points mentioned above.

This guide is available at http:/ /medical-vending.com/privacy

Any modifications to the guide will take effect on the address above. Next to each chapter title we also display the appropriate law and regulation reference.

GLOSSARY

1. *those who are concerned/User:* any private individual who can be identified – directly or indirectly – based on any specified, personal data;
2. *private data:* information concerning an individual that can be made public, especially his name, identification number, one or more physical, physiological, mental, financial, cultural or social identifier and deductions that can be made based on that information;
3. *unique data:*

- private information concerning racial, ethnic origins, political opinion or party membership, religious or other ideologies, union membership, sexual orientation.
- information about medical conditions, substance abusing or police record;

4. *consent:* the voluntary and explicit display of the user's will, based on adequate notification and which provides unambiguous consent to the management of his private information in general or for certain operations;
5. *objection:* a statement of the user which objects against the treatment of his private information and requests the cancellation of the data management and the deletion of the data;
6. *data manager:* a private or corporate personality or a body with no legal corporate personality status, which independently or in association with others determines the

data management, is responsible for the decisions concerning operations (including used devices), and executes them through his designated data processor;

7. *data management:* in general, – independent of the nature of any procedure – any operation or sum of operations on the private data, including their collection, recording, saving, listing, organizing, storing, editing, downloading, transmission, publication, coordination, attachment, lockup, deleting or destruction, also the disabling of further access to the data, creation of image, voice or video recording, or recording data enabling physical identification (fingerprints, DNA samples, etc.);
8. *data transmission:* allowing a third party to access the data;
9. *publication:* making the data public, and thus accessible to anyone;
10. *data deletion:* rending the data incomprehensible in a way that their restoration is not possible;
11. *data designation:* placing a certain identifier on the data;
12. *data lockup:* identification of the data to limit its usage for a defined or unlimited period of time;
13. *data elimination:* the physical destruction of the media device on which the data is stored;
14. *data processing:* technical tasks connected to the data management processes, independent of the applied methods and devices, the location, the only factor is whether the task is being done on the private data;
15. *data processor:* a private or corporate personality or an body with no legal corporate personality status, which, according to contracts signed between him and the data manager carries out the data processing;
16. *data responsible:* an organization carrying out public tasks, which produced electronic, compulsory to publish data, or during whose operation such data was created;
17. *data publisher:* an organization carry out public tasks, which, in case the data responsible fails to publish the data, publishes the data he received on the internet;
18. *database:* the sum of data present in an account;
19. *third party:* a private or corporate personality, or a body with no corporate personality, who is not among the users, data managers or data processors.

LEGAL CLAIM FOR DATA MANAGEMENT

1. 1. Private information can be managed, if
- the user provided his consent, or
- the law or – by legislative authorization in a determined area – the local council orders the management due to public interest.

2. Private information can also be managed, if obtaining the consent of the user proves to be impossible or would require undue cost or effort, and the private data management

   a) is necessary for the fulfillment of legal liabilities of the data manager, or

   b) is required for the fulfillment of legal liabilities of the data manager or a third person and this interest is proportional enough to limit the protection of private information.

3. In case the concerned is unable to act or due to insuperable circumstances cannot provide his consent, than for the sake of his personal protection or the protection of another and in case there is a direct threat to the personal safety, physical wellbeing, property or in order to avoid such an action, personal data may be managed, to the extent in which the imminent danger can be stopped.
4. A user above the age of 16 does not need the written approval of his legal guardian when consenting to the management of his data.
5. If the purpose of the voluntarily data management is the fulfillment of a written contract with the data manager, the contract must contain all relevant information concerning data handling that the user should be aware of, especially the specification of types of data involved, the time period of data management, the purpose of data collection, the transmission of data, its recipients, the involvement of a data processor. The contract should unambiguously contain that the user consents to the management of his data as set out in the contract with his signature.
6. If the recording of the private data is done with the consent of the user, the manager, with the recorded data – unless otherwise regulated by legislation

- for fulfillment of his legal liabilities
- is required for the fulfillment of legal liabilities of the data manager or a third person and this interest is proportional enough to limit the protection of private information, can continue to manage the data without the further need for consent from the user, even if the user decides to withdrawn his approval.

PURPOSE OF DATA COLLECTION

1. Private data can only be managed for a well-defined purpose, exercising rights and for fulfilling legal responsibilities. In all stages of the data management, it should be according to its defined purpose, the recording and handling of data should be fair and legal.
2. Only those private information should be used that are crucial for the fulfillment of the purpose of the data management and enables the goal to be reached. Private data can only be used for achieving the goal, to an appropriate extent and time.

OTHER DATA MANAGEMENT PRINCIPLES

Private data remains private during the data management up until its connection with the user can be reestablished. Connection can be reestablished, if the data processor has the necessary technical requirements available to him.

During data management, their accuracy, wholeness and – if required for the purposes of the data management – their up to date state must be ensured along with that the user can only be identified during the time period of the data management.

REGISTRATION ON THE WEBSITE

1. According to Act CXII, 20. § (1) of 2011 on Informational Self-determination and Freedom of Information, the followings should be states in connection with data management during a registration to a website:
- The fact that private data is being recorded,
- Defining who is affected
- Purpose of the data collection
- Duration of the data management
- The responsible for data management who comes in contact with the private data during his work,
- Notifying the users about their legal rights concerning data management.

2. An alert that data collection is taking place, the defined data types involved: User name, password, family and surname, email address, sex, company data, phone number, address, date of registration, IP address used for registration.
3. The group of affected: All who register on the website.
4. Purpose of data collection: The service provider manages the users private data for the following reasons:
- access to all features of the website, service providing
- access to private areas (distributor pages)
- registration for events
- joining a Webinar
- offering a newsletter service.

5. Duration of data management, date of deletion of the data: Simultaneously with the deletion of the registration.
6. Person responsible for data management who will come in contact with private data: Private data will be managed by sales and marketing employees, honoring the guidelines set out above.
7. Notifying the users of their data management rights: You can request the deletion or modification of your private data through the following ways:
- via mail to IVM Zrt. 72-100. Berényi street Bld 22,, Székesfehérvár, 8000.
- via email to support@ivm.hu.

8. Legal grounds for data management: With the consent of the user, according to Infotv. 5. § (1), and the law regulating electronic trader services and services connected to information society (hereinafter: Elker tv.) 13/A. § (3):

   For the purposes of providing a service, the provider can manage private data that are technically crucial for the service providing. The service provider must, in all cases, choose the processes that he operates during the service providing connected to the informational society, if not other conditions are interfering, that the management of private information should only takes place if it is crucial for the service providing and for the fulfillment of other obligations set out in the law, and even in this case only to a reasonable extent and duration.

FUNCTIONAL DATA MANAGEMENT PRINCIPLES

1. When billing costs resulting from the service providing in connection with the informational society, the provider can manage the private data connected with the service, such as address, date of the service providing to the user, duration and location.
2. For the purposes of providing a service, the provider can manage private data that are technically crucial for the service providing. The service provider must, in all cases, choose the processes that he operates during the service providing connected to the informational society, if not other conditions are interfering, that the management of private information should only takes place if it is crucial for the service providing or for other purposes defined by Elker and even in these cases only to a reasonable extent and duration.
3. The service provider can only use the private data connected to the service of other reasons – such as service quality improvement, sending electronic advertising material or other mail, market research – if the purpose was previously defined and the affected gave his consent.
4. The user must retain the right to stop the data management during any stage in the collection and the service.
5. The managed private data must be deleted in case no contract is signed, a contract expires or after an invoice was sent. Data must be deleted if the data management is cancelled or the user wishes it to be deleted. Unless regulated otherwise by law, the data deletion must be completed right away.
6. The service provider must make information accessible to the user prior and during the service concerning exactly what data types are managed and for what purposes, including data not directly connected to the user.

COOKIE HANDLING

1. According to Act CXII, 20. § (1) of 2011 on Informational Self-determination and Freedom of Information, the following must be stated concerning the cookie handling of a website:

- the fact of the data collection,
- Defining who is affected
- Purpose of the data collection
- Duration of the data management
- The responsible for data management who comes in contact with the private data during his work,
- Notifying the users about their legal rights concerning data management.

2. For the usage of ‘password protected processes using cookies’ and ‘security cookies’, there is no need to ask for the prior consent of the user.
3. The fact of data management and its extent: unique identification numbers, dates, time.
4. Affected: Every visitor of the website.
5. Purpose of management: identification of users, identifying individual users, tracking visitors.

6. Duration of data management and deadline of their deletion: The data management done by the session cookies ends upon the end of the webpage visit.
7. Data processor who can come in contact with private data: By using cookies the data processor does not access any private data.
8. Notifying the users of their data management rights: Users have the option to delete the cookies in their browser, usually under Tools/Options, Privacy settings.
9. Legal grounds of data management: Consent of the user is not required as long as the cookies are exclusively used to transmission of information within a network or if it essential for the service providing of the subscriber or the internet provider.
10. The webpage visit data is monitored using Google Analytics by the Provider. During this service, data might be transferred. This data is not suitable for identification. For Google's privacy statement, follow http://www.google.hu/policies/privacy/ads/.
11. The webpage uses Google Adwords remarketing codes. Using this service, the Google Network and Google Display Network can offer relevant advertisement to visitors who previously have used the website. Remarketing codes use cookies to track visitors. Users can block these cookies and access more information about Google's policies at http://www.google.hu/policies/technologies/ads/ and https://support.google.com/analytics/answer/2700409.

CONTACT DATASHEET

1. According to Act CXII, 20. § (1) of 2011 on Informational Self-determination and Freedom of Information, the following must be stated concerning the message sending done on the contact datasheet and its handling:
- the fact of the data collection,
- Defining who is affected
- Purpose of the data collection
- Duration of the data management
- The responsible for data management who comes in contact with the private data during his work,
- Notifying the users about their legal rights concerning data management.

2. The fact of data collection and the boundaries of managed data: Name, email address, date of filling out datasheet, IP address.
3. The group of the affected: Those who fill out the datasheet.
4. Purpose of data collection: The service provider manages the data of the customers to enable contact between them.
5. Duration of data management and deadline for their deletion: The data manager retains the data until the fulfillment of the service.
6. Person responsible for data management who will come in contact with private data: Private data will be managed by sales and marketing employees, customer service honoring the guidelines set out above.
7. Notifying the users of their data management rights: You can request the deletion or modification of your private data through the following ways:
- via mail to IVM Zrt. 72-100. Berényi street Bld 22, Székesfehérvár, 8000.
- via email to support@ivm.hu.

8. Legal grounds for data management: The consent of the user and Infotv. 5. § (1).

NEWSLETTER, DM OPERATION

1. According to law XLVIII. of 2008, 6. §, concerning the basic principles and limitations of business advertisement activates, the user can consent prior to receiving marketing offers, other packages from the Provider on the address given during registration.
2. Furthermore the Customer, with keeping the basic principles of this document in mind, can consent to the management of his private data by the Provider for the sending of marketing material.
3. The Provider cannot send unwanted marketing material and the user has an unlimited right to cancel the sending of any such material without providing a reason. In this case the Provider must delete all private data associated with the sending of marketing material from his database and will not approach the user with further offers. The user can unsubscribe from the messages by clicking on a link within them.
4. According to Act CXII, 20. § (1) of 2011 on Informational Self-determination and Freedom of Information, the following must be stated concerning the newsletters:

- the fact of the data collection,
- Defining who is affected
- Purpose of the data collection
- Duration of the data management
- The responsible for data management who comes in contact with the private data during his work,
- Notifying the users about their legal rights concerning data management.

5. The fact of data collection and the boundaries of managed data: Name, email address, date and time.
6. The group of the affected: Those who subscribe to the newsletter.
7. Purpose of data collection: sending marketing materials to customers containing notification of new information, products, sales, new features, etc.
8. Duration of data management and deadline for their deletion: until and upon unsubscribing from the newsletter.
9. Person responsible for data management who will come in contact with private data: Private data will be managed by sales and marketing employees, honoring the guidelines set out above.
10. Notifying the users of their data management rights: The user can unsubscribe from the newsletter anytime and without a charge.
11. The newsletter service utilizes the following data processor:

    MiniCRM Plc.

    13-14., Madách Imre street, Budapest, 1075

    E-mail: help@minicrm.hu

    Phone: 06 (1) 999-0402

12. Legal ground for managing data: the voluntarily consent of the user and law XLVIII. of 2008, 6. § (5), concerning the basic principles and limitations of business advertisement activates, that states:

    The advertiser, advertisement service provider – during the period consented to – can store the private data of the users consented to receive such services. This data – that of the recipient – can only be used and stored for the defined purposes, until that is fulfilled, and can only be transferred to another party with the consent of the user.

FACEBOOK

1. According to Act CXII, 20. § (1) of 2011 on Informational Self-determination and Freedom of Information, the data transmission of the website must be stated according to:
- the fact of the data collection,
- Defining who is affected
- Purpose of the data collection
- Duration of the data management
- The responsible for data management who comes in contact with the private data during his work,
- Notifying the users about their legal rights concerning data management.

2. The fact of data collection and the boundaries of managed data: Facebook.com social website username and the users public profile.
3. The group of the affected: Those who are registered Facebook users and have liked the webpage.
4. Purpose of data collection: On the Facebook.com webpage, sharing or liking certain features of the website, including products, sales.
5. Duration of data management the person responsible for data management who will come in contact with private data: About the source of the data collection, the method of transmission and the legal claims, turn to http://www.facebook.com/about/privacy.
6. As the data management is done on Facebook.com, about the duration of the management, options to modify or delete data, turn to:
- (http://www.facebook.com/legal/terms?ref=pf),
- (http://www.facebook.com/about/privacy/)

7. Legal basis: the voluntarily consent of the user to the management of his private data on Facebook.com

DATA MANAGEMENTS

1. According to Act CXII, 20. § (1) of 2011 on Informational Self-determination and Freedom of Information, the data transmission of the website must be stated according to:
- the fact of the data collection,

- Defining who is affected
- Purpose of the data collection
- Duration of the data management
- The responsible for data management who comes in contact with the private data during his work,
- Notifying the users about their legal rights concerning data management.

2. The fact of data collection and the boundaries of managed data: All personal data collected on the website.
3. The group of the affected: All website users.
4. Purpose of data collection: Operation of the website.
5. Duration of data management, deadline for deletion: Upon the request of the concerned.
6. The person, company responsible for data management, who will come in contact with private data: The following party will handle the data with the above mentioned conditions:

   IVM Zrt

   Berényi út 72-100, Bld 22. Berényi street, Székesfehérvár, 8000

   Email: info@ivm.huTel: +36 (22) 300-893

   And

   Maxer Kft.
   9024 Győr, Répce u. 24.
   Email: info@maxer.hu
   Tel: +3612579913

   GTC: https://maxer.hu/aszf.html
7. Notifying the users of their data management rights: You can request the deletion of your private data with the internet provider.
8. Legal basis: the voluntarily consent of the user Legal grounds for data management: The consent of the user, Infotv. 5. § (1) and Act CVIII. of 2011 on Electronic Business Services and Services Connected to the Informational Society (especially 13/A. §)

DATA SECURITY

1. The data manager plans and executes the data processing with respect to the private sphere of the users.
2. The data manager is responsible for the security of the data, including its protection and enable the adherence to Info tv and other data protection regulations.
3. The data manager protects the data from unauthorized access, editing, forwarding, publishing, deletion, deletion, damage or loss due to accidents, turning unreachable due to changing technical circumstances.
4. Enables by the necessary technical solutions that prevent the data contained in the database to be directly connectable to the users, except when such connection is required by law.

5. During the automatic management of the data, the data manger and data processor ensures, with the following actions to:
- Prevent unauthorized data input;
- Prevent unauthorized access to the automatic data management system through a data input equipment;
- Enable the traceability and monitoring of personal data with a tracking device in order to whom said data was transmitted or could be transmitted;
- Enable the traceability and monitoring of what personal data was inserted into the automatic management system and by whom;
- The restorability of the of the system in case of a failure in the equipment;
- Enable error reporting during the automatic data processing.

6. The advancement of technical levels must be followed at all times by the data manager and processor when determining and applying data security measures. Between two data management methods, the more secured one must be selected except if its places un unreasonable burden on the data manager.

RIGHTS OF THE CONCERNED

1. Those concerned can request from the Service provider information about the management of their private data and can request its modification or – expect for compulsory data management – their deletion.
2. Upon a request the data manager must provide information about the data, the data processed by the data processor, their source, the purpose of the data management, the legal claims, time period, the name and address of the data processor, other works concerning the data alongside with – in case of forwarding the private data of the user – the legal claims for the forwarding and the addressee.
3. The data manager creates a log and records data forwarding in order to inform the user and to ensure the legal grounds, which contains the date of the forwarding, the legal claim and the addressee, the exact extant of the private data forwarded as well as other information defined in laws and regulations concerning data forwarding.
4. After notifying the Service provider of the request, it must return these information in writing as soon as he can but no later than 30 days after, in a clear, understandable form. This information cannot be charged.
5. The Service provider upon, the request of the user, provides information about the data managed, their source, the purpose of data management, the legal claim, the length, the name of the data processor, his address, any activities connected to data processing alongside with – in case of forwarding private information – the legal claim for data forwarding and the addressee. After notifying the Service provider of the request, it must return these information in writing as soon as he can but no later than 30 days after, in a clear, understandable form. This information cannot be charged.
6. The Service provider, in case the private information is not valid and an accurate one is accessible, can correct the data.
7. Instead of deleting the data, the Service provider can lock it up, in case the user requests this, if, based on the information available, the deletion would be against the user's interest. Locked up data can only be managed until the data management purpose is still valid and which disabled the deletion of the data.

8. The Service provider deletes the data if its management is against the law, upon user request, of the data is incomplete or inaccurate – and this cannot be corrected in a legal manner – but only if the deletion is allowed by the law, the purpose of the data management is fulfilled, the managing period has expired or if ordered by a court or the Hungarian National Authority for Data Protection and Freedom of Information agency.
9. The data manager tags the private data if the concerned disagrees with its validity of accuracy but this fact cannot be proven.
10. Modifications, locking up, tagging and deletion of data must be reported to the concerned and all those to whom the data was forwarded. This is not compulsory if according to the purposes of the data management it is not against the legal interest of the user.
11. If the data manager does not fulfill the request of the user to modify, lock up or delete his data, within 30 days of receiving the request in writing it must return a written explanation, citing the reasons of noncompliance. He also needs to notify the user possible legal remedies such as turning to a court or the Agency.

LEGAL REMEDY

1. The user can object against the handling of his private data if,
- the management of private data or its forwarding is necessary for the fulfillment of legal obligations of the Provider, or for the fulfilling of legal claims of the Provider or a third party, except if ordered by legislation;
- the management of private data or its forwarding is done for direct marketing gains, polling or scientific research;

2. or in other cases regulated by the law.
3. After receiving the objection the Provider must investigate it as soon as possible or no later than in 15 days, must decide on its merit and inform the user of its decision in writing. If the Provider decides to comply with the objection and stops the data management – including the recording of new data and its forwarding – locks up the data it needs to inform all parties concerned who have access to or received the data and they also need to comply to the request.
4. If the user is not satisfied with the decision of the Provider, – within 30 days of receiving it, he has the option to turn to the court which will handle the case out of turn.
5. In case of infringement, the user can turn to Hungarian National Authority for Data Protection and Freedom of Information agency.

   1125 Budapest, Szilágyi Erzsébet fasor

   Address: 1530 Budapest, mailbox: 5.

   Phone: +36 -1-391-1400

   Fax: +36-1-391-1410

   E-mail: ugyfelszolgalat@naih.hu

COURT ENFORCEMENT

1. The fact that the data management is lawful must be proved by the data manager. The legal claim for the data forwarding must be proven by the receiver.
2. Coming up with a verdict is the responsibility of the court. The case – according to the wishes of the concerned – can be opened at the local court of his residence.
3. The court case can involve parties with not legal capacity. The Agency can be involved in the case on the side of the prevailing party.
4. If the court rules in favor of the user, the data manager must provide the requested information, modify the data, lock it up, delete it, stop the automatic data processing, must respect the user's rights and return the data forwarded.
5. If the court rejects the request of the data receiver, the data manager must delete the private data of the user within 3 days. The data manager is obliged to delete the data even if the recipient fails to turn to the court.
6. The court can order the publishing of its ruling along with the public identification of the data manager if the data security and a wider range of concerned parties interest demand it.

COMPENSATION AND REMEDIES

1. If the data manager causes damages by mishandling the data or not respecting data security regulation, he must pay compensations.
2. If the data manager violates the users right by mishandling the data or not respecting data security regulation, he must pay grievance fees to the wronged party.
3. The data manager must cover damages caused for the concerned and the grievance fees if he violated the user's legal rights. The data manager is exempt from these if he can prove that the damage or violation was not connected to the data managing process and was an inevitable and came from another source.
4. Damages and grievances are not to be paid if they are a direct result of the purposeful or reckless behavior of the user.

CLOSING REMARKS

While creating this guide we took into consideration the following regulations:

- Act CXII. of 2011 – on Informational Self-determination and Freedom of Information (Infotv.)
- Act CVIII. of 2011 – on Electronic Business Services and Services Connected to the Informational Society (especially 13/A. §)
- Act XLVII. of 2008 – on prohibition of unfair treatment of consumers;
- Act XLVIII. of 2008, on the basic public marketing practices and limitations
- (especially 6.§)
- Act XC. of 2005, on Freedom of Information
- Act C. of 2003, on Electornic News reporting (especially 155.§)

- 16/2011. EASA/IAB advise on online marketing behavior advertisement practices