Otterworks.online

Privacy Policy

In brief

Personal data are collected and handled in accordance with the law.

DM letter is sent only in the case of specific consent. System messages, however, can be sent without specific consent.

Personal data are stored as secure as possible.

Personal data are given to a third party only with User consent.

Anyone can be given information on the data stored considering him/her or the deletion of personal data asked on any of our availability.

Introduction

The **OtterWorks Ltd.** (registration number: 01-09-991920, tax number: 24131951-2-41, site: 1031 Budapest, Vízimolnár utca 18. 2. em. 7.) (henceforward: Service Provider, Data Manager) subdues itself under the following policy.

Chapter (1) § 20 of Act CXII of 2011 on information self-determination right and freedom of information states that those concerned (user of the website in the present case: User henceforward) have to be informed prior to starting data management whether this data management is **based on consent** or it is compulsory.

User has to be informed clearly and in detail regarding all facts related to the management of his/her data prior to starting data management. Special attention has to be paid to the **aims and legal bases** of data management, the **person entitled to data management and processing** and the **time interval of** data management.

User has to be informed based on chapter (1) § 6 of the Act on information on that personal data can be managed if obtaining the consent of the concerned person is impossible or would require disproportionate costs

- it is required for completing legal obligations related to the data manager or
- required for enforcing the rightful interest of the data manager or a third party and the enforcement of these interests is proportional to the limitation of the privacy protection right.

This privacy policy information has to cover the rights of those concerned in relation to data management and the possibilities of legal redress as well.

In case the personal data of those concerned is not possible or would require extremely high costs (as in the present case in a website), giving information is also possible via publishing the information as well:

a) the fact that data are collected,
b) list of those concerned,
c) aim of data collection,
d) time constraints of data management,
e) possible data managers entitled to know the data,
f) rights and legal redress possibilities of those concerned in data management together with
g) The registry number of data management in case there is a place for registering data management in data protection.

The present privacy policy guide regulates privacy of the following websites: http://otterworks.online and is based on the above specification. Information can be obtained from http://otterworks.online/privacy.html

Modifications to the data become effective when they appear on the webpage above. After each chapter heading of this guide the reference to the law also appear.

Explanatory terms *(3.§)*

1. *concerned/User:* natural person identified or can be identified – directly or indirectly – based on any particular personal data;
2. *personal data*: any data that can be related to the User – especially the name, username of the User and any knowledge characteristic for one or more physical, physiological, mental, economic, cultural, or social identity of the User – and any conclusion related to the User drawn from the data;
3. *data manager:* the natural or legal entity or organization without legal personality that determines individually or together with others the aim of data management, concludes and implements or have decisions related to data management executed by the data processor charged by him/her/it.
4. *data management*: any measure or measure series made in relation to the data independent from the applied method, especially collection, record, ordering, storage, modification, query, forwarding, publication, harmonization or connection, blocking, deletion and destruction and impeding the further use of data, preparing photo, sound or film record and recording the physical characteristics suitable for the identification of the person (e.g. fingerprint, palm print, DNA sample, iris photo);
5. *data processing*: performing technical measures related to data management procedures independent from the method and device applied to performing the procedures, also independent from the place of application given that the technical task was performed on the data;
6. *data processer*: the natural or legal entity or organisation without legal personality, who based on a contract made with the data manager – including contract made on the basis of legal regulations – performs the processing of data;
7. *dataprotection incident*: unlawful usage or processing of personal data, especially unauthorized access, modification, forwarding, publishing, deleting, or accidental annihilation and lesion

Messaging, contact

1. Based on chapter (1) § 20 of Act CXII of 2011 on informatic self-determination right and the freedom of information the following has to be determined regarding the operation of the registration on the website of:

   a) the fact of data collection,
   b) the range of users,
   c) the aim of data collection,
   d) the time period of data management,
   e) the potential data managers entitled to know the data,
   f) giving data on the rights of the Users related to data management.

2. Fact data collection, the range of managed data and the aim of data management:

Personal data	**Aim of data management**
Name, e-mail address	Contact maintaining, identification.
Date of messaging	The fulfillment of technical operation.
IP address at time of messaging	The fulfillment of technical operation.

3. Range of those involved: Every user who has sent message/made a request on the website.

4. Time period of data management, deadline of data deletion: Right away after the accomplishment of administration.

5. Possible data managers entitled to know the data: Personal data can be managed by the staff of the data manager respecting the above principles.

6. Giving information on the rights of Users related to data management: Deletion or modification of personal data can be initiated by the User as follows:

   - By post at the address: 1031 Budapest, Vízimolnár utca 18. 2. em. 7.
   - Via e-mail: hello@otterworks.online

7. The datas of the data processer (storage service), which was enlisted in the data processing:

   EZIT Kft.
   1132 Budapest, Victor Hugo u. 18-22. V. em 5021.
   info@ezit.hu
   +36 1 700 40 30

8. Legal base of data management: Consent of the User, chapter (1) § 5 of the Act on information.

Data management in relation with applications

1. Based on chapter (1) § 20 of Act CXII of 2011 on informatic self-determination right and the freedom of information the following has to be determined regarding the operation of the registration on the website of:

   a) the fact of data collection,
   b) the range of users,
   c) the aim of data collection,
   d) the time period of data management,
   e) the potential data managers entitled to know the data,
   f) giving data on the rights of the Users related to data management.

2. Fact data collection, the range of managed data and the aim of data management:

Personal data	**Aim of data management**
Name, e-mail address	Contact maintaining, identification.
Date of messaging	The fulfillment of technical operation.
IP address at time of messaging	The fulfillment of technical operation.

3. Range of those involved: Every user of the application.

4. Time period of data management, deadline of data deletion: Right away after the deletion of the registration/request of the deletion from the user.

5. Possible data managers entitled to know the data: Personal data can be managed by the staff of the data manager respecting the above principles.

6. Giving information on the rights of Users related to data management: Deletion or modification of personal data can be initiated by the User as follows:

   - By post at the address: 1031 Budapest, Vízimolnár utca 18. 2. em. 7.
   - Via e-mail: hello@otterworks.online

7. The datas of the data processer (storage service), which was enlisted in the data processing:

   EZIT Kft.
   1132 Budapest, Victor Hugo u. 18-22. V. em 5021.
   info@ezit.hu
   +36 1 700 40 30

8. Legal base of data management: Consent of the User, chapter (1) § 5 of the Act on information.

9. In the applications, every application store (typically GooglePlay, iTunes, App Store, WinStore, etc.) manages the happening data requirements for acquisitions according to their own privacy policy.

Use of Cookies

1. Based on chapter (1) § 20 of Act CXII of 2011 on information self-determination right and on freedom of information the followings have to be determined in relation to the use of cookies on the website of the website:

   a) the fact of data collection,
   b) the range of Users,
   c) the aim of data collection,
   d) the time period of data management,
   e) the potential data managers entitled to know the data,
   f) giving data on the rights of users related to data management.

2. The fact of data collection, range of managed data: individual identification number, dates, times.

3. The range of users: All Users visiting the website.

4. The aim of data collection: identification of Users and the monitoring of the visitors.

5. The time period of data management and the deadline of deletion of data: Time period of data management in the case of session cookies lasts until the termination of visiting the website.

6. The potential data managers entitled to know the data: Personal data is not managed by the data manager with the use of cookies.

7. Giving information on the rights of the Users related to data management: Users can delete cookies in the Tools/Settings menu of the browser generally at the menu item Data protection.

8. Legal base of data management: No consent is required in case the sole aim of using cookies is to pass data via electronic messenger networks or if Service Provider needs the data for providing services related to the information society asked for by the User.

Use of Google Adwords conversion following

1. The data processer uses the „Google AdWords" online commercial program, and it makes use of the Google's conversion following service. The Google conversion following is the Google Inc.'s analyst service (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; „Google").

2. When the User reaches a website via a Google-advertisement, a necessary conversion following cookie gets on the computer. The validity of these cookies are restricted, and they do not contain any personal data, this way a User can not be identified by them.

3. When the User searches specific pages of a website , and the cookie is not expired, then the Google and the data processer can see too that the User has clicked on an advertisement.

4. Every Google AdWords client gets another cookie, then these cookies can not be followed through the websites of the AdWords client.

5. The informations - which were got by the conversion follower cookies - provides conversion statistics for the clients of AdWords conversion following. The clients get informations this way about the number of the users, who has clicked on their advertisement and about "conversion follower" signed sites. But they do not get informations, which can be used for identifying any user.

6. If you do not want to take part in the conversion following, you can decline it, if you block the possibility of the setup of the cookies. After that you will not be in the conversion following statistics.
7. Further information on the privacy Policy of Google can be read at http://www.google.hu/policies/privacy/ads/

The service of Google Analytics

1. This website uses the service of Google Analytics, which is the webanalyser service of the Google Inc. („Google"). The Google Analytics uses so called „cookies", textiles, which are saved on your computer, and they help the analysis of the website usage of the Users.

2. The cookies of the websites which were visited by the User and their connecting informations are sent and stored on one of the Google's servers in the USA. With the activation of the IP-anonymisation on the websites the Google can shorten the time of the IP-anonymisation of the Users in the European Union or in the member states of the European Economic Region.

3. Only in unique cases the full IP-addresses are sent to the servers of Google in the USA and they get shorten there. Operators of these websites commit the Google to use these informations for interpretations about the usage of the website, furthermore to create reports about the activity of the website, and to do their website and internet usage related duties.

4. In the Google Analytics, the forwarded IP-address of the Users will not be matched with others data by the Google. The store of the cookies can be prevented in the settings of the web browsers, but in this way it can happen, if some features of the websites will not work. You can prevent Google from collecting datas about the website usage habits of the users (including IP-addresses too), if you download and setup this web browser plugin. https://tools.google.com/dlpage/gaoptout?hl=hu

Newsletter, DM activity

1. According to § 6 of Act XLVIII of 2008 on the fundamental conditions of economic advertising activity the User may give consent in advance to the Service Provider for sending him/her advertisement and other consignment via the addresses given at registration.

2. Furthermore, the User may give consent to the Service Provider for managing the personal data for sending advertisements bearing in mind the regulations of the present guide.

3. Service Provider sends no unwanted advertisement and the User has the option to unsubscribe the sending of advertisements without any limitations and justification. In such case the Service Provider deletes every information – required for sending the messages – from the register and sends no further offers. User can unsubscribe the sending of advertisement by clicking on the link in the message.

4. Based on chapter (1) § 20 of Act CXII of 2011 on information self-determination right and on freedom of information the followings have to be determined in relation to newsletter sending data management:

   a) the fact of data collection,
   b) the range of users,
   c) the aim of data collection,
   d) the time period of data management,
   e) the potential data managers entitled to know the data,
   f) giving data on the rights of the Users related to data management.

5. The fact of data collection, range of managed data: name, e-mail address, (telephone number), date, time.

6. The range of users: All Users subscribing for the newsletter.

7. The aim of data collection: sending electronic messages containing advertisements (e-mail, SMS, push notification) to the User giving information on actual products, discounts, new functions, etc.

8. The time period of data management and the deadline of deletion of data: until the withdrawal of the consent, i.e. unsubscribing from the newsletter.

9. The potential data managers entitled to know the data: Personal data can be managed by the staff of the data manager in respect for the above principles.

10. The registration number of the data management: NAIH-114714/2017.

11. Giving information on the rights of the Users related to data management: Users can unsubscribe from the newsletter at any time at no cost.

12. The data processer enlisted in data management:

    The Rocket Science Group, LLC
    675 Ponce de Leon Ave NE
    Suite 5000
    Atlanta, GA 30308 USA

13. Legal base of data management: voluntary consent of the User, chapter (1) § 5 of the Act on information and chapter (5) § 6 of Act XLVIII of 2008 on the fundamental conditions and limits of economic advertisement activity:
    The advertiser, advertisement provider and the advertisement publisher – in the range determined in the consent – holds a register of the personal data of people giving consent to them. Data given in this register – related to the recipient of the advertisement – can be managed according to the consent declaration until its withdrawal and can be passed to a third party only with the consent of the User in advance.

Community websites

1. Based on chapter (1) § 20 of Act CXII of 2011 on information self-determination right and on freedom of information the followings have to be determined in relation to the community sites:

    a) the fact of data collection,
    b) the range of Users,
    c) the aim of data collection,
    d) the time period of data management,
    e) the potential data managers entitled to know the data,
    f) giving data on the rights of the Users related to data management.

2. The fact of data collection, range of managed data: name and public profile image of the User registered at Facebook/Google+/Twitter/Pinterest/YouTube/Instagram etc.

3. The range of Users: All Users registered at Facebook/Google+/Twitter/Pinterest/YouTube/Instagram etc. and gave like to the website.

4. The aim of data collection: sharing and giving like to certain content of the website, its products, sales or the website itself.

5. The time period of data management, the potential data managers entitled to know the data and giving information on the rights of the Users related to data management: User can obtain more information regarding the source of data, their management, the method and legal base of the passing of data at the website itself. Data management is carried out at the community sites, therefore the time period and

method of data management, the deletion and modification possibilities of data are regulated by the terms and conditions of the community site.

6. Legal base of data management: voluntary consent of the User for the management of personal data at community sites.

User services and other data management

1. If you have question during using some of the services of the data processor, or the User has some problem you can get in contact with the data processer on the website (on phone, e-mail, community sites, etc.).

2. The data processer deletes the incoming e-mails, messages, on phone, on Facebook, etc. what contains the name and e-mail address or any other given personal information of the User, after 2 years from the start of the service.

3. We give information about the privacy policy which is not in this guide at the start of the service.

4. For exceptional magisterial request, or in case of law accumulation the service provider is bound for guidance, information providing, transferring, or making documents available for these organisation.

5. In these cases the service provider only gives personal informations for the request (if they pointed out the exact aim and the necessary informations) what are essentials for the aim of the request.

Data security (7.§)

1. Data manager is obligated to plan and execute data management procedures so that the protection of the private sphere of the Users is ensured.

2. Data manager and in the course of its activity the data processor are obligated to provide the security of the data (with passwords or antivirus programs). They are also obligated to take the technical and organisational measures and form the procedure regulations required for Info tv., or enforcing the Act of information and other data and secret security regulations.

3. Data have to be protected using the appropriate measures especially against

    - illegal access
    - modification

- passing
- publication
- deletion or destruction
- accidental destruction or damage
- inaccessibility as a result of changing the applied technology.

4. Applying the adequate technical solution it has to be ensured that data stored in the registry cannot be connected to each other and cannot be related to the User.

5. In the course of illegal access, modification and illegal publication or use of personal data the data manager and processor ensures with further measures:

    - about the forming and operating of a proper information technological and technical environment
    - about the monitored choice and control of the fellow workers who participate in the service
    - about the publish of detailed operation, risk managing and utilizing services

6. On the bases of above, the service provides that the managed data:

    - is available for the entitled
    - the authenticity and authentication is insured
    - uniformity can be confirmed

7. The informational system of the data processer and storage provider protects against:

    - deceit of computer technology
    - spying
    - virus
    - spams,
    - hacks
    - other attacks.

User rights (14.-19.§)

1. The User has the right to request the Service Provider to give information on the management of personal data. User can also request the correction of his/her personal data and also for the deletion or blocking of the personal data – except for compulsory data management.

2. In reply to the request the data manager gives information on the processed data of the User, their source managed and processed by the data processor, the aim, legal base of data management, the name, address and data management activity of the data processor and on the legal base and recipient of the data in case of data passing.

3. Data manager keeps a register of data passing in order to legality control and to give information to the User. The register contains the time, legal base and recipient of personal data passing together with the type of personal data passed and other data the determination of which is found in the legislation prescribing data management.

4. The data manager makes a register about data transferring, because of informing the User and to monitor the lawfulness of the data transferring. This register contains the date of the passing of the personal datas, the aim of it, the recipient, the range of the personal datas, and the other informations what are necessary because of the law.

5. Upon request from the User the Service Provider gives information regarding the data, their source managed by him/her, also the aims, legal bases, time period, name, address and activity of the potential data processor associated with data processing. Service Provider has to ask any request as soon as possible but no later than 25 days of the submission of the request in writing. The information is free of cost.

6. Service Provider in case his/her personal data are not real but real personal data are available for the data manager it may replace personal data.

7. Service Provider blocks the personal data instead of deleting them in case the User asks for it or based on the available information it would threat the legal interest of the User. Blocked personal data can be managed only until the data management aim has not been over stepped.

8. Service Provider deletes the personal data if its management is illegal, the User requests the deletion, the managed data are deficient or inaccurate – and this condition cannot be corrected legally – provided that deletion is not precluded by the law, the aim of data management terminated, or the time period of data storage determined by the law has passed, or deletion of the data was ordered by the court or by the Hungarian National Authority for Data Protection and Freedom of Information.

9. Data manager marks the personal data if the User debates their correctness or accuracy but the correctness or accuracy of the controversial data cannot be determined clearly.

10. In the case of correcting, blocking, marking or deleting personal data the User and everyone to whom the data were passed for management have to be notified. Notification can be omitted if this does not interfere the interest of the User regarding the purpose of data management.

11. In case the data manager does not perform the correction, blocking or deletion request of the User the data manager has to issue the reasons and legal bases of rejecting the correction, blocking or deletion request in writing, within 25 days of receiving the request. In the case of rejecting the correction, deletion or blocking request the data manager informs the User on the possibilities of legal redress and authority complaint.

Legal redress

1. User may complain against the treatment of his/her personal data if
   a) management and passing of personal data are necessary solely for completing legal obligations related to the Service Provider or necessary for enforcing the legal interest of the Service Provider, the data receiver or a third party except for it was ordered by the data management law;
   b) use or passing of personal data are made for directly obtaining business, public opinion research or scientific research;
   c) in other cases determined by the law.

2. Service Provider studies the complaint within 15 days at the most from the submission of the request and decides regarding the founding of the request informing the requester in writing on the decision. If the Service Provider states the correct founding of the complaint of the User, data management is terminated – including further data collection and passing – and data are blocked and inform all of those to whom personal data affected by the complaint were passed earlier and who are obligated to take measures in order to enforce the right of complaint on the complaint and the measures based on it.

3. In case the User should not agree to the decision of the Service Provider he/she can turn to court – within 30 days of the publication of the decision. The court has to consider the case out of turn.

4. Complaint regarding the possible breaching of the law by the data manager can be made to the Hungarian National Authority for Data Protection and Freedom of Information:

   Hungarian National Authority for Data Protection and Freedom of Information
   1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Postal address: 1530 Budapest, P.O.Box: 5.
Telephone: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

Enforcement of rights on court (22.§)

1. Data manager is obligated to prove that data management is in accordance with the law. Legal data passing has to be proved by the data receiver.

2. Judgement of the legal action is the authority of the court. Legal action can be initiated – according to the opinion of the User – on courts in the location of either the residence or the dwelling of the User.

3. Party in the legal action can be someone who has no legal capacity in the legal action. Authority may interfere into the legal action in the interest of the success of the User.

4. In case the court supports the request, it obligates the data manager to give the information, correct, block or delete the data, to eliminate the decision made using automated data processing, to account with the complaint right of the User and to give out the data requested by the data receiver.

5. In case the court rejects the request of the data receiver the data manager is obligated to delete the personal data of the User within 3 days of issuing the verdict. Data manager is obligated to delete the data even if the data receiver does not take on court within the given time limit.

6. The court may order the publication of its verdict – with publishing the identification data of the data manager as well – if data protection interests and the protected rights of a greater number of Users require.

Compensation and complaint refund(23. §)

1. In case the data manager caused loss to someone by illegal management of User data or breaching the requirements of data security he/she is obligated to refund the loss.

2. In case the data manager offends the personality right of the User by illegal management of his/her data or by breaching the data security requirements the User is entitled to request complaint refund. Data manager is exempted from responsibility of loss or from the payment of the complaint refund if he/she proves that the loss or damage of the personality right of the User was caused by an unavoidable reason outside the sphere of data management.

3. Refund for loss or complaint refund have not to be paid if the loss or damage was caused by the deliberate or significantly careless behaviour of the User.

Closing remarks

The following regulations were accounted in the course of composing the guide:

- Act CXII of 2011 – on information self-determination and the freedom of information;
- Act CVIII of 2001 – on electronic trade services and certain issues of services related to the information society (mainly § 13/A);
- Act XLVII of 2008 – on prohibiting dishonest trade practice against consumers;
- Act XLVIII of 2008 – on the fundamental conditions and certain limitations of economic advertisement activity (especially § 6);
- Act XC of 2005 – on the freedom of electronic information;
- Act C of 2003 - on electronic information (especially § 155);
- Opinion 16/2011 – on the EASA/IAB directive related to the adequate practice of behaviour based online advertisement
- The recommendation of the Hungarian National Authority for Data Protection and Freedom of information about the previous data protection requirements