Anker Business Center, Anker köz 2-4
H-1061 Budapest
Hungary
www.healcloud.com

Privacy Policy

Last updated: October 12, 2019

At Healcloud, we respect your concerns about privacy and value the relationship that we have with you. Like many companies, we use technology and material means to collect information that helps us enhance your experience and our products and services. However, we have also minimized the use of technological tools to the minimum necessary in order to reach our goals of providing you with the best possible services as our users. We do not use Google analytics, cookies, newsletters or any trackers on our website and do not engage in data transfers to third countries.

Please take a moment to familiarize yourself with this privacy policy and let us know if you have any questions by contacting us via e-mail. We may update this Privacy Policy from time to time, depending on new apps or products we release, mandatory law changes or in accordance with our corporate privacy strategy. Please review the Privacy Policy periodically for any changes.

The processing of personal data, such as the name, address, e-mail address, or telephone number of a data subject shall always be in line with the General Data Protection Regulation (GDPR), and in accordance with the country-specific data protection regulations applicable to Healcloud. By means of this privacy policy, our enterprise would like to inform the general public of the nature, scope, and purpose of the personal data we collect, use and process. Furthermore, we use this to inform data subjects of the rights to which they are entitled.

1. Definitions

Healcloud's Privacy Policy uses the terms used by the European legislator for the adoption of the General Data Protection Regulation (GDPR). Our Privacy Policy aims to be legible and understandable for the general public, as well as our customers and business partners. To ensure this, we would like to first explain the terminology used:

a) Personal data
Personal data means any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

b) Data subject
Data subject is any identified or identifiable natural person, whose personal data is processed by the controller responsible for the processing.

c) Processing
Processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection,

recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

d) Restriction of processing
Restriction of processing is the marking of stored personal data with the aim of limiting their processing in the future.

e) Profiling
Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

f) Pseudonymisation
Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

g) Controller or controller responsible for the processing
Controller or controller responsible for the processing is the natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

h) Processor
Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

i) Recipient
Recipient is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

j) Third party
Third party is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and other persons who, under the direct authority of the controller or processor, are authorised to process personal data.

k) Consent

Consent of the data subject is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

l) Data Protection Officer (DPO)
The function within our firm in charge of implementing the Privacy Strategy of the company and the main interface between data subjects and the firm in enforcing their rights at their request.

m) GDPR
GDPR is the abbreviation for the General Data Protection Regulation.

2. Data protection principles

Healcloud is committed to processing data in accordance with its responsibilities under the GDPR. To that end, Article 5 of the GDPR requires personal data to be:

a) processed **lawfully**, **fairly** and in a **transparent** manner in relation to individuals;
b) collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed;
d) **accurate** and, where necessary, **kept up to date;** every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept 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 longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

3. Rights of the data subject

Under the GDPR, data subjects have been granted a series of rights related to their personal data. The following will list and explain these rights as detailed by the regulation. Healcloud has introduced organizational and technical measures to ensure that all these rights can be fulfilled at the request of each data subject.

a) Right of confirmation

Each data subject shall have the right granted by the European legislator to obtain from the controller the confirmation as to whether or not personal data concerning him or her are being processed. If a data subject wishes to avail himself of this right of confirmation, he or she may, at any time, contact the DPO of Healcloud.

b) Right of access
Each data subject shall have the right granted by the European legislator to obtain from the controller free information about his or her personal data stored at any time and a copy of this information. Furthermore, GDPR grants the data subject access to the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;
- the existence of the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

Furthermore, the data subject shall have a right to obtain information as to whether personal data are transferred to a third country or to an international organisation. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

If a data subject wishes to avail himself of this right of access, he or she may, at any time, contact our DPO.

c) Right to rectification
Each data subject shall have the right granted by the European legislator to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

If a data subject wishes to exercise this right to rectification, he or she may, at any time, contact the DPO of Healcloud.

d) Right to erasure (Right to be forgotten)

Each data subject shall have the right granted by the European legislator to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies, as long as the processing is not necessary:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws consent to which the processing is based according to point (a) of Article 6(1) of the GDPR, or point (a) of Article 9(2) of the GDPR, and where there is no other legal ground for the processing.
- The data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.
- The personal data have been unlawfully processed.
- The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.
- The personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

If one of the aforementioned reasons applies, and a data subject wishes to request the erasure of personal data stored by Healcloud, he or she may, at any time, contact the DPO of the company. The DPO shall promptly ensure that the erasure request is complied with in due time, according to the GDPR requirements.

Where the controller has made personal data public and is obliged pursuant to Article 17(1) to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers processing the personal data that the data subject has requested erasure by such controllers of any links to, or copy or replication of, those personal data, as far as processing is not required. The DPO of Healcloud will arrange the necessary measures applicable in each individual case.

e) Right of restriction of processing

Each data subject shall have the right granted by the European legislator to obtain from the controller restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests instead the restriction of their use instead.
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.
- The data subject has objected to processing pursuant to Article 21(1) of the GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

Anker Business Center, Anker köz 2-4
H-1061 Budapest
Hungary
www.healcloud.com

If one of the aforementioned conditions is met, and a data subject wishes to request the restriction of the processing of personal data stored by Healcloud, he or she may at any time contact our DPO. Our DPO will arrange the restriction of the processing id applicable and necessary.

f) Right to data portability
Each data subject shall have the right granted by the European legislator, to receive the personal data concerning him or her, which was provided to a controller, in a structured, commonly used and machine-readable format. He or she shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, as long as the processing is based on consent pursuant to point (a) of Article 6(1) of the GDPR or point (a) of Article 9(2) of the GDPR, or on a contract pursuant to point (b) of Article 6(1) of the GDPR, and the processing is carried out by automated means, as long as the processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Furthermore, in exercising his or her right to data portability pursuant to Article 20(1) of the GDPR, the data subject shall have the right to have personal data transmitted directly from one controller to another, where technically feasible and when doing so does not adversely affect the rights and freedoms of others.

g) Right to object
Each data subject shall have the right granted by the European legislator to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her, which is based on point (e) or (f) of Article 6(1) of the GDPR. This also applies to profiling based on these provisions.

Healcloud shall no longer process the personal data in the event of the objection, unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

If Healcloud processes personal data for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing. This applies to profiling to the extent that it is related to such direct marketing. If the data subject objects to Healcloud to the processing for direct marketing purposes, Healcloud will no longer process the personal data for these purposes.

In addition, the data subject has the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her by Healcloud for scientific or historical research purposes, or for statistical purposes pursuant to Article 89(1) of the GDPR, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

In order to exercise the right to object, the data subject may contact the DPO of Healcloud. In addition, the data subject is free in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, to use his or her right to object by automated means using technical specifications.

h) Automated individual decision-making, including profiling
Each data subject shall have the right granted by the European legislator not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her, as long as the decision (1) is not is necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) is not authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or (3) is not based on the data subject's explicit consent.

If the decision (1) is necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) it is based on the data subject's explicit consent, Healcloud shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and contest the decision.

If the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may, at any time, contact the DPO of Healcloud. As part of our commitment to minimize personal data processing to only what is necessary, at Healcloud, we do not engage in automated individual decision-making, including profiling.

i) Right to withdraw data protection consent
Each data subject shall have the right granted by the European legislator to withdraw his or her consent to processing of his or her personal data at any time.

If the data subject wishes to exercise the right to withdraw the consent, he or she may, at any time, contact our DPO.

4. Collection of general data and information on the website

Our website collects a series of general data and information when a data subject or automated system calls up the website. This general data and information are stored in the server log files. We may collect the following metadata:
(1) the browser types and versions used
(2) the operating system used by the accessing system
(3) the website from which an accessing system reaches our website (so-called referrers)
(4) the sub-websites
(5) the date and time of access to the Internet site
(6) an Internet protocol address (IP address)

(7) the Internet service provider of the accessing system
(8) any other similar data and information that may be used in the event of attacks on our information technology systems.

When using these general data and information, Healcloud does not draw any conclusions about the data subject. Rather, this information is needed to: (1) deliver the content of our website correctly
(2) optimize the content of our website as well as its advertisement
(3) ensure the long-term viability of our information technology systems and website technology, and
(4) provide law enforcement authorities with the information necessary for criminal prosecution in case of a cyber-attack.

Therefore, we analyze anonymously collected data and information statistically, with the aim of increasing the data protection and data security of our enterprise, and to ensure an optimal level of protection for the personal data we process. The anonymous data of the server log files are stored separately from all personal data provided by a data subject.

5. Contact possibility via the website

Our website contains information that enables a quick electronic contact to our enterprise, as well as direct communication with us, which also includes a general address of the so-called electronic mail (e-mail address). If a data subject contacts the controller by e-mail or via our contact form, the personal data transmitted by the data subject are automatically stored. This data may include name, surname, email address and Internet Protocol (IP) address of a data subject. Such personal data transmitted on a voluntary basis by a data subject to the data controller are stored solely for the purpose of processing or contacting the data subject. There is no transfer of this personal data to third parties.

6. Legal basis for the processing

Art. 6(1) lit. a GDPR serves as the legal basis for processing operations for which we obtain consent for a specific processing purpose. If the processing of personal data is necessary for the performance of a contract to which the data subject is party, as is the case, for example, when processing operations are necessary for the supply of goods or to provide any other service, the processing is based on Article 6(1) lit. b GDPR.

The same applies to such processing operations which are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services. If our is company subject to a legal obligation by which processing of personal data is required, such as for the fulfilment of tax obligations, the processing is based on Art. 6(1) lit. c GDPR. In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person. This would be the case, for example, if a visitor were injured in our company and his name, age, health insurance data or other vital information would have to be

passed on to a doctor, hospital or other third party. Then the processing would be based on Art. 6(1) lit. d GDPR.

Finally, processing operations could be based on Article 6(1) lit. f GDPR. This legal basis is used for processing operations which are not covered by any of the abovementioned legal grounds, if processing is necessary for the purposes of the legitimate interests pursued by our company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Such processing operations are particularly permissible because they have been specifically mentioned by the European legislator. He considered that a legitimate interest could be assumed if the data subject is a client of the controller (Recital 47 Sentence 2 GDPR).

Where the processing of personal data is based on Article 6(1) lit. f GDPR our legitimate interest is to carry out our business in favor of the well-being of all our employees and the shareholders.

7. Routine erasure and blocking of personal data

As a data controller, we shall process and store the personal data of data subjects only for the period necessary to achieve the purpose of storage, or as far as this is granted by the European legislator or other legislators in laws or regulations to which the controller is subject to.

If the storage purpose is not applicable, or if a storage period prescribed by the European legislator or another competent legislator expires, the personal data are routinely blocked or erased in accordance with legal requirements.

8. Period for which the personal data will be stored

The criteria used to determine the period of storage of personal data is the respective statutory retention period. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfilment of the contract or the initiation of a contract.

9. Confidentiality and security of your personal data

We consider the confidentiality and security of your information to be of the utmost importance. We will use industry standard physical, technical and administrative security measures to keep your personal data confidential and secure and will not share it with third parties, except as otherwise provided in this Privacy Policy, or unless such disclosure is necessary in special cases, such as a physical threat to you or others, as permitted by applicable law.

However, because the Internet is not a 100% secure environment, we cannot effectively guarantee the absolute security of personal data, and there is some risk that an unauthorized third party may find a way to circumvent our security systems or that transmission of your information over the Internet will be intercepted. It is your

responsibility to protect the security of your login information. Please note that e-mails communications are typically not encrypted and should not be considered secure.

10. Compliance measures taken by Healcloud

To prove our commitment to privacy, we have taken a series of operational and technical measures to introduce all GDPR principles in our operations and product suite. For further details about our internal processes and policies, we kindly invite you to contact our DPO.

Lawful, fair and transparent processing
a. To ensure its processing of data is lawful, fair and transparent, Healcloud reviews its data mapping and processes at least annually.
b. Individuals have the right to access their personal data and any such requests made to Healcloud are dealt with in a timely manner, according to the timeframe set by the regulation and to the Privacy policies within the firm.

Lawful purposes
a. All data processed by Healcloud are done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. Healcloud notes the appropriate lawful basis in the data mapping.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in Healcloud's systems.

Data minimisation
Healcloud ensures that personal data collected are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This is why we decided not to use Google Analytics and cookies on our website and not to collect any more data than what is absolutely necessary for the well-functioning of our website.

Accuracy
a. Healcloud takes reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Storage / Erasure
a. To ensure that personal data is not kept for longer than necessary, Healcloud puts in place storage limitations for each category of personal data and review their status and the process annually.
b. The storage policy considers what data should/must be retained, for how long, and why.

Security
a. Healcloud ensures that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data is limited to personnel who need access and appropriate security should be in place to avoid unauthorized sharing of information.
c. When personal data is deleted, this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions will be set-up in place.

Breach
In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, Healcloud shall promptly assess the risk to people's rights and freedoms and, if appropriate and necessary, report this breach to the Data Protection Authority, which will be done according to the internal Data Breach policy.

11. Data protection provisions about the application and use of Facebook

On the website, the controller has integrated components of the enterprise Facebook. Facebook is a social network.

A social network is a place for social meetings on the Internet, an online community, which usually allows users to communicate with each other and interact in a virtual space. A social network may serve as a platform for the exchange of opinions and experiences, or enable the Internet community to provide personal or business-related information. Facebook allows social network users to include the creation of private profiles, upload photos, and network through friend requests.

The operating company of Facebook is Facebook, Inc., 1 Hacker Way, Menlo Park, CA 94025, United States. If a person lives outside of the United States or Canada, the controller is the Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

With each call-up to one of the individual pages of this Internet website, which is operated by the controller and into which a Facebook component (Facebook plug-ins) was integrated, the web browser on the information technology system of the data subject is automatically prompted to download display of the corresponding Facebook component from Facebook through the Facebook component. An overview of all the Facebook Plug-ins may be accessed under
https://developers.facebook.com/docs/plugins/.
During the course of this technical procedure, Facebook is made aware of what specific sub-site of our website was visited by the data subject.

If the data subject is logged in at the same time on Facebook, Facebook detects with every call-up to our website by the data subject-and for the entire duration of their stay on our Internet site-which specific sub-site of our Internet page was visited by the data subject. This information is collected through the Facebook component and associated with the respective Facebook account of the data subject. If the data subject clicks on

one of the Facebook buttons integrated into our website, e.g. the "Like" button, or if the data subject submits a comment, then Facebook matches this information with the personal Facebook user account of the data subject and stores the personal data.

Facebook always receives, through the Facebook component, information about a visit to our website by the data subject, whenever the data subject is logged in at the same time on Facebook during the time of the call-up to our website. This occurs regardless of whether the data subject clicks on the Facebook component or not. If such a transmission of information to Facebook is not desirable for the data subject, then he or she may prevent this by logging off from their Facebook account before a call-up to our website is made.

The data protection guideline published by Facebook, which is available at https://facebook.com/about/privacy/, provides information about the collection, processing and use of personal data by Facebook. In addition, it is explained there what setting options Facebook offers to protect the privacy of the data subject. In addition, different configuration options are made available to allow the elimination of data transmission to Facebook. These applications may be used by the data subject to eliminate a data transmission to Facebook.

12. Data protection provisions about the application and use of LinkedIn

The controller has integrated components of the LinkedIn Corporation on this website. LinkedIn is a web-based social network that enables users with existing business contacts to connect and to make new business contacts. Over 400 million registered people in more than 200 countries use LinkedIn. Thus, LinkedIn is currently the largest platform for business contacts and one of the most visited websites in the world.

The operating company of LinkedIn is LinkedIn Corporation, 2029 Stierlin Court Mountain View, CA 94043, UNITED STATES. For privacy matters outside of the UNITED STATES LinkedIn Ireland, Privacy Policy Issues, Wilton Plaza, Wilton Place, Dublin 2, Ireland, is responsible.

With each call-up to one of the individual pages of this Internet site, which is operated by the controller and on which a LinkedIn component (LinkedIn plug-in) was integrated, the Internet browser on the information technology system of the data subject is automatically prompted to the download of a display of the corresponding LinkedIn component of LinkedIn. Further information about the LinkedIn plug-in may be accessed under https://developer.linkedin.com/plugins. During the course of this technical procedure, LinkedIn gains knowledge of what specific sub-page of our website was visited by the data subject.

If the data subject is logged in at the same time on LinkedIn, LinkedIn detects with every call-up to our website by the data subject—and for the entire duration of their stay on our Internet site—which specific sub-page of our Internet page was visited by the data subject. This information is collected through the LinkedIn component and associated with the respective LinkedIn account of the data subject. If the data subject clicks on one of the LinkedIn buttons integrated on our website, then LinkedIn assigns

this information to the personal LinkedIn user account of the data subject and stores the personal data.

LinkedIn receives information via the LinkedIn component that the data subject has visited our website, provided that the data subject is logged in at LinkedIn at the time of the call-up to our website. This occurs regardless of whether the person clicks on the LinkedIn button or not. If such a transmission of information to LinkedIn is not desirable for the data subject, then he or she may prevent this by logging off from their LinkedIn account before a call-up to our website is made.

LinkedIn provides under https://www.linkedin.com/psettings/guest-controls the possibility to unsubscribe from e-mail messages, SMS messages and targeted ads, as well as the ability to manage ad settings. LinkedIn also uses affiliates such as Eire, Google Analytics, BlueKai, DoubleClick, Nielsen, Comscore, Eloqua, and Lotame. The setting of such cookies may be denied under https://www.linkedin.com/legal/cookie-policy. The applicable privacy policy for LinkedIn is available under https://www.linkedin.com/legal/privacy-policy. The LinkedIn Cookie Policy is available under https://www.linkedin.com/legal/cookie-policy.

13. Updating the Policy

Please note that we review our privacy practices from time to time, and that these practices are subject to change. Any change, update, or modification will be effective immediately upon posting on our Site. We will notify you of any material change to this Privacy Policy by posting a notice on our Site's homepage for a reasonable period of time following such update, and by changing the effective date (located at the top of this page). Be sure to return to this page periodically to ensure familiarity with the most current version of this Privacy Policy.

14. Name and Address of the controller

Controller for the purposes of the General Data Protection Regulation (GDPR), other data protection laws applicable in Member states of the European Union and other provisions related to data protection is:

Heacloud Kft
Anker Business Center, Anker köz 2-4
H-1061, Budapest, Hungary
Website: www.healcloud.com

15. Name of the data protection officer

At this point, the data protection officer function of our firm is accomplished by:

Ioana Stupariu
ioana.stupariu@healcloud.com