

PRIVACY POLICY

Holospital Kft.

Effective from: 1st December 2023

Last modified: 1st December 2023

Thank you for using our services! Holospital Kft. protects Your personal data and respects Your rights related thereto.

To achieve the above goals present privacy policy (hereinafter as: **"Policy"**) in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter as: **"GDPR"**) contains all information regarding the processing of personal data provided to

Company name: **Holospital Korlátolt Felelősségű Társaság**

Short name: **Holoindustry Kft.**

Registered seat: **3530 Miskolc, Avasalja utca 13.**

Company registration number: **05-09-032686**

Tax number: **27911484-2-05**

EU VAT: **HU27911484**

Registered at: **Metropolitan Court of Miskolci as Company Registration Court**

Represented by: **Zsolt Mihályfi as managing director**

E-mail: info@holospit.al

(hereinafter as: **„Service Provider"**)

by persons (hereinafter referred to as: **"User"**) as data subjects in connection with the use of the collaborative online 3D visualization platform and medical image diagnostic software named Holospital (hereinafter as: **„Software"**) operated by the Service Provider and made available for use under the terms and conditions set out in the Service Provider's end user license agreement (hereinafter referred to as: **"EULA"**) and for other purposes specified in this Policy.

The Software may be freely downloaded by the User from the Microsoft Store or is made available to the User through other channels.

The Service Provider draws the User's attention to the fact that with respect to the personal data that the User uploads or provides within the Software and the scope of which is not determined by the Service Provider, the Service Provider is considered a data processor, with regard to which it is the User's obligation and responsibility to obtain the necessary consent from the data subjects for the transfer of the data or the processing of the data by the Service Provider.

The aim of the Policy is to give a clear picture about why, how and how long we process personal data of individuals who come into contact with our company.

I. A few data privacy related definitions to better understand the Policy

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.

Processing

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

Controller

means 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 EU or Member State law.

Processor

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

Third Party

means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

Data forwarding

Means the disclosure of personal data to specific third parties.

Data Subject

Everybody who shares his/her personal data with the Service Provider through the Website or via other channels or whose personal data is processed by the Service Provider otherwise. For example, You, who reads this Policy.

Consent of the data subject

means 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.

Sensitive data

personal data referring to racial origin, nationality, political opinions or membership in any political party, religious or other beliefs, membership of an advocacy organization, sex life, personal data concerning health, pathological data.

Genetic data

means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Biometric data

means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.

Personal data breach

means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Most of the above definitions are used by the GDPR. The full text of the GDPR is available at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN> The above list is not complete so should you need more information or explanation do not hesitate to contact us.

We would like to inform You that during our processing we do not process or request from You any sensitive, genetic or biometric data.

II. Other definitions

Login interface

mean the interface under the domain name "organizationname.holospital.al" provided by the Service Provider for the User's organization (employer, customer, client) to register for the use of the Software and to access the Software

IP address

short for Internet Protocol address, it is a series of numbers that uniquely identifies the computers and mobile devices of users accessing the Internet. IP addresses can even be used to geographically locate a visitor using a particular computer. The address of the pages visited, as well as the date and time of the visit, are not in themselves suitable for identifying the data subject, but when combined with other data (e.g. data provided during registration) they can be used to draw conclusions about the user.

Licensee

means the legal person or other entity without legal personality with whom the Service Provider has entered into a license agreement for the Software, typically the User's employer or client

Registration

means the process of entering personal data in the Login Interface, as detailed below in this Policy, whereby the User creates his/her own personal profile, protected by a password.

Website

means the website under the domain <https://holospital.it/>

III. Principles of data processing

The Service Provider shall process the personal data of the User or of the Data Subject in accordance with the following principles laid down in Article 5 Section (1) of the GDPR:

- processes personal data lawfully and fairly and in a transparent manner ("**lawfulness, fairness and transparency**");
- collects personal data only for specified, explicit and legitimate purposes and does not process them in a way incompatible with those purposes ("**purpose limitation**");
- the personal data processed are adequate, relevant and limited to what is necessary for the purposes for which they are processed ("**data minimisation**");
- ensure that the personal data are accurate and, where necessary, kept up to date and take all reasonable steps to ensure that personal data which are inaccurate for the purposes for which they are processed are erased or rectified without undue delay ("**accuracy**");
- store the personal data 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 ("**limited storage**");
- process personal data in a manner to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by implementing appropriate technical or organisational measures ("**integrity and confidentiality**")

IV. In which cases do we process personal data?

The Service Provider shall process the personal data of the User or the Data Subject in the following cases, taking into account the principles described in Chapter III above:

- Browsing the Website
- Registration for the Software;

- Contacting, customer service
- Cookies

V. Which data, for which purpose and for how long do we process?

In each of the cases set out above, the legal ground for processing personal data may be:

- In accordance with article 6 Section (1) Point a) of the GDPR the freely given, specific, informed and unambiguous consent of the User and the Data Subject (hereinafter as: „**Consent**“).
- In accordance with article 6 Section (1) Point b) of the GDPR processing is necessary for the performance of a contract to which the User is party (hereinafter as: „**Performance of Contract**“).
- In accordance with article 6 Section (1) Point c) of the GDPR processing is necessary for compliance with a legal obligation to which the controller is subject (hereinafter as: „**Compliance**“).
- In accordance with article 6 Section (1) Point f) of the GDPR processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (hereinafter as: „**Legitimate Interest**“).

V.1. Browsing the Website

Scope of data processed	Purpose of processing	Legal ground of processing	Naming the legitimate interest	Duration of processing
IP address of the Data Subject	Protection of the IT systems of the Service Provider and securing the Website / Login Interface	Legitimate interest	Securing the operation of the Website	30 days from the last visit

The Website and the Login Interface may be freely visited and browsed by the Data Subject without expressly providing any personal data to the Service Provider. However, when visiting the Website or the Login Interface at any time, the Data Subject's computer or mobile device sends a request to the Service Provider. It is like sending a letter to which You wish to get the content of the Website or the Login Interface as an answer. The Service Provider can only answer this request if the Data Subject provides his/her address. This address is the Data Subject's internet identifier address, IP address for short. The Service Provider sends the requested Website to this IP address. This is an automatic process, by typing the domain of the Website or the Login Interface to the web browser or by clicking to a link published anywhere that is directing to the Website or the Login Interface the Data Subject gives his/her consent to provide the IP address for this purpose and to be processed

by the Service Provider. To make this „correspondence” smooth the servers of the Service Provider store the IP address of the Data Subject in log files.

The identification and storing of IP addresses is necessary to protect the IT systems of the Service Provider and the Website as well. Protection against possible malicious activities against the Website is partly ensured by that the Service Provider is logging the operation of the Website and the Login Interface and in this log, it lists the IP addresses from which requests to its servers were made. If the Service Provider detects an activity from an IP address that interferes with the secure operation of the Website, he addresses will be blacklisted. Any malicious activity is prevented and resolved through legal action. If nothing extraordinary occurs, the Service Provider deletes the log files and the IP addresses. IP addresses stored in log files will not be used by the Service Provider for any other purpose and will be automatically deleted within 30 days and we keep it only if the Data Subject has performed any prohibited activity from that IP address. These activities are either listed above or other activities that violate local, state, national or international law.

V.2. Registration

Scope of data processed	Purpose of processing	Legal ground of processing	Duration of processing
First and last name of the User	Identifying the User, creating a user account	Performance of contract	Until the expiry of the User's licence or until the User's organisation sends a request for cancellation
E-mail address of the User	Identifying the User, creating a user account	Performance of contract	Until the expiry of the User's licence or until the User's organisation sends a request for cancellation
Login name set by the User	Identifying the User, creating a user account, login to account	Performance of contract	Until the expiry of the User's licence or until the User's organisation sends a request for cancellation
Password set by the User	Identifying the User, creating a user account, login to account	Performance of contract	Until the expiry of the User's licence or until the User's organisation sends a request for cancellation
Professional medical qualification of the User	Identifying the User, creating a user account, use of the Software, verification that the User is duly authorised to use the Software	Performance of contract	Until the expiry of the User's licence or until the User's organisation sends a request for cancellation

The use of the Software is subject to Registration and the creation of a user account, i.e. in order to use the Software and access the functions of the Software, the User must create a user account by means of Registration. This requires the provision of the above information.

It is important for the User to keep safe the data provided during Registration, in particular the password. The protection of this data is also the responsibility of the User, and the Service Provider shall not be liable for any loss or unauthorised access to this data by the User. After Registration, the User is obliged to notify the Service Provider if the security of his/her account has been compromised or if his/her login details have been compromised

V.3. Contacting, customer service

In order to provide Users with information about the Software and the services available through the Software, the Service Provider maintains a customer service. Customer service requests are managed via e-mail. Users and Data Subjects may contact the Service Provider through the latter channel if they have any questions regarding the Software or the use of the service available through it.

If the User or Data Subject contacts the Service Provider via the e-mail address info@holospit.al, the following data must be processed in order for the Service Provider to be able to fulfil the (customer service) request with appropriate quality assurance:

Scope of data processed	Purpose of processing	Legal ground of processing	Naming the legitimate interest	Duration of processing
First and last name of the User / Data Subject	Identification of the User / Data Subject fulfilment of (customer) support request	Performance of contract (in case of an existing business relationship) / Legitimate interest (without business relationship)	The Service Provider's legitimate interest in providing its service to an adequate standard or in establishing a new business relationship with the User.	Until an objection is raised by the User / Data Subject but for quality assurance until 31 st December of the year following the year in which the (customer service) request was resolved
E-mail address of the User / Data Subject	Identification of the User / Data Subject fulfilment of (customer) support request	Performance of contract (in case of an existing business relationship) / Legitimate interest	The Service Provider's legitimate interest in providing its service to an adequate standard or in	Until an objection is raised by the User / Data Subject but for quality assurance until 31 st December of the year following the

		(without business relationship)	establishing a new business relationship with the User.	year in which the (customer service) request was resolved
The social media contact of the User / Data Subject possibly shared in his/her e-mail „signature“	-	Performance of contract (in case of an existing business relationship) / Legitimate interest (without business relationship)	The Service Provider's legitimate interest in providing its service to an adequate standard or in establishing a new business relationship with the User.	Until an objection is raised by the User / Data Subject but for quality assurance until 31 st December of the year following the year in which the (customer service) request was resolved

The Service Provider requests the User and the Data Subject not to provide the Service Provider with any other personal data in addition to the above, especially if the Service Provider does not expressly request it. The Service Provider shall immediately and irrevocably delete any personal data provided to it by the User or the Data Subject without being requested to do so and shall not be liable in connection with any data thus obtained.

VI. What are cookies and why we use them?

Cookies are data packages that are sent by our webserver to Your computer automatically, where they are stored – depending on the type of the cookie – for a definite period of time.

Cookies do not hold any security risk to Your computer or not cause any malfunction.

In order to ensure the smooth operation of the Website and the Service, certain cookies (known as session cookies) are automatically installed on Your computer when You visit the Website and the platform through which the Service is available. The purpose of such cookies is to ensure the security of the Website and the Service, to preserve the data recorded on our online forms, to display multimedia content and to balance the traffic on the Website and the platform through which the Service is made available. Personal data collected through the use of these cookies (in particular the IP address of Your computer) will be processed for our legitimate interest in the safe and smooth operation of the Website for the duration of Your stay on our Website and/or during the use of the Service. Closing Your browser will automatically delete them from Your computer.

With Your consent given on the Website and on the platform through which the Service is made available, the following types of cookies may be installed on Your computer for the following purposes:

- Technically necessary session cookies: without which the site would simply not function, these are needed to identify You as a User, for example to manage whether you have logged in, etc. This is typically a session ID, the rest of the data is stored on the server, which is more secure. There is a security aspect, if the session cookie "value" is not generated correctly then there is a risk of session hijacking attack, so it is imperative that these values are generated correctly. Other terminology calls session cookies all such cookies that are deleted when you close the browser (a session is a browser session from start to exit).
- Cookies for web analytical measurements and for statistical purposes (e.g., Google Analytics). These are important to us because we are provided with information about the specific characteristics of our visitors (IP address, city, type of device, browser, operating system You are using, and what sub-pages You have visited on our site). We use these data anonymized for statistics and reports to improve the Website our marketing strategy.

For more information on Google Analytics cookies visit:

<https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage>

- Remarketing cookies (such as Google AdWords) allow us to analyze how You use our site and, consequently, to display personalized content to You, including advertising on online platforms outside our site (e.g., other websites or social media).

For more information on Google Adwords cookies visit:

<https://support.google.com/adwords/answer/2407785?hl=hu>

In addition, we distinguish between session-specific cookies and persistent cookies. A cookie valid for a single session only survives until the User closes the browser. Permanent cookies continue to live and are not automatically deleted when You close Your browser. Why do they stay there and what's good about it? Well, such persistent cookies, for example, help to make the site run faster and remembering things that the User has set for himself/herself on the Website.

Accepting or authorizing the use of cookies is not mandatory. You can reset your browser settings to reject all cookies or to indicate when a cookie is being sent You can also manage cookies in your browser settings. How you set them depends on the type of browser you use.

You may find information on cookie settings for the most popular browsers on the following link:

- Google Chrome: https://support.google.com/chrome/answer/95647?hl=hu-hu&p=cpn_cookies
- Firefox: <https://support.mozilla.org/hu/kb/sutik-informacio-amelyet-weboldalak-tarolnak-szami>

- Internet Explorer / Edge: <https://support.microsoft.com/hu-hu/help/17442/windows-internet-explorer-delete-manage-cookies>
- Safari: <https://support.apple.com/hu-hu/HT201265>

During the visit to the Website, the Service Provider may record and process the following data about the Data Subject as a visitor to the Website and the device used for browsing:

- IP address of the device used by the visitor,
- the type of browser used,
- the characteristics of the operating system of the device used for browsing (e.g. language setting),
- time of visit,
- the subpages visited, feature or services used,
- clicks

VII. How can You withdraw Your consent if the ground for processing is based on consent?

If under present Policy the legal ground of processing is the consent of the Data Subject, then the Data Subject has the right to withdraw this consent. Depending on the purpose of processing there are many ways to do it. You may withdraw Your consent given at browsing at any time, free of charge and without limitation by revisiting the Website and clicking on the pop-up window. In addition, if You do not have the possibility to withdraw Your consent this way, you may withdraw it by sending a message to info@jholospita.al or a mail sent to the Service Provider's registered seat address or in case of newsletter subscription by clicking on the "Unsubscribe" button at the bottom of the email.

Please note that the withdrawal of consent does not affect the lawfulness of the data processing prior to the withdrawal.

VIII. Where and how my personal data is stored?

All personal data is stored electronically on secure, reliable servers.

VIII.1. Website hosting.

The Service Provider informs the Data Subject that the server used for storing the Website and the data provided through the Website during the visit is the Service Provider's own internal server located in Hungary, so no data is transferred to third parties in this regard.

VIII.2. Data storage related to software operation

VIII.2.1. Data storage by Licensee

If, under the agreement between the Service Provider and the Licensee, the Software is running on the Licensee's own servers and is accessed via the Licensee's internal network, the Service Provider shall not store any data relating to the User or transmit such data to third parties. The Service Provider informs the User, however, that the Service Provider has remote access to the Licensee's systems for the purpose of providing technical assistance to the Licensee and the User in connection with the Software and its operation, during which it may access the User's data to the extent necessary, but may only perform such data processing operations with the permission or on the basis of instructions from the Licensee and/or the User, and therefore may not change or delete the data at its own discretion.

The same shall apply when using the desktop version of the Software.

VIII.2.2. Data storage by the Service Provider

If the Software is not installed on the Licensee's servers, the Service Provider may use the following third party service providers for cloud storage and operation of the Software, which are European partners and, in accordance with the provisions of the GDPR, the following service providers established in the European Union for the processing of data of European data subjects. The specific service provider indicated below will be selected by agreement between the Service Provider and the Licensee, of which the Licensee is obliged to inform the User, however, in case of a request by the User to the Service Provider, the Service Provider will also provide the User with information.

VIII.2.2.1. Microsoft Azure

- Company name: **Microsoft Ireland Operations Limited**
- Registered seat: **One Microsoft Place, South County Business Park, Leopardstown, Dublin 18., Ireland**
- Registration number: **256796**
- Represented by: **Anna Sheehan CEO**
- Phone: **+353 1 706 3117**
- Online contact: <https://privacy.microsoft.com/en-us/privacy-questions>
- European Data Centers: **Cienna, Brussels, Milan, Amsterdam, Copenhagen, Helsinki, London, Berlin, Frankfurt, Magdeburg, Geneva, Zürich, Madrid, Stavanger, Warsaw, Athens, Gävle, Staffanstorp (Malmö), Paris, Marseille, Dublin**
(hereinafter as: **"Microsoft"**)

Microsoft processes and controls data of residents of the European Union within the territory of the European Union in Ireland. However, Microsoft may also transfer data to its parent company Microsoft Corporation, in which case the User's data will still be secure and protected by the provisions of the GDPR in view of the European Commission's EU-US Data Flow Compliance Decision.

Microsoft's privacy policy and other related documents are available here:

<https://privacy.microsoft.com/en-us>

<https://privacy.microsoft.com/en-us/privacystatement>

<https://support.office.com/hu-hu/article/az-adatvédelmi-beáll%C3%ADtások-megtekintése-a-microsoft-office-adatvédelmi-központjában-d672876e-20d3-4ad3-a178-343d044e05c8?omkt=hu-HU&ui=hu-HU&rs=hu-HU&ad=HU>

VIII.2.2.2. Amazon AWS

- Company name: **Amazon Web Services, Inc. EMEA SARL**
- Registered seat: **38 Avenue John F. Kennedy, Luxembourg, Luxembourg**
- Registration number: **B 186284**
- E-mail: EU-privacy-DSR@amazon.com
- Represented by: **Eva Gehlin and Barbara Scarafia directors**
- European Data Centers: **London, Frankfurt, Stockholm, Paris, Dublin**
(hereinafter as: **"Amazon"**)

Although the Service Provider uses Amazon's servers located in the European Union, the parent company of Amazon is a service provider located outside the European Union in the United States of America, so some data may be transferred outside the European Union. Nevertheless, your data is still safe and protected by the provisions of the GDPR in light of the European Commission's EU-US Data Flow Compliance Decision.

Amazon ensures the protection of data on multiple levels, physically protecting data storage servers, its infrastructure through uninterruptible power supplies and other advanced tools, limiting access to data, continuous monitoring of its system, encryption, and finally, environmentally selecting data center locations, because Amazon set up its data centers in places where it is not exposed to nature, such as seismic activity. More information about Amazon's security solutions is available at <https://aws.amazon.com/compliance/data-center/data-centers/>

Amazon has the following security and privacy certifications: https://aws.amazon.com/compliance/programs/?nc1=h_ls

Amazon's general privacy policy can be reached at: <https://aws.amazon.com/privacy/>

VIII.2.2.3. Google Cloud Platform

- Company name: **Google Ireland Ltd**
- Registered seat: **Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland**
- Registration number: **368047**
- Represented by: **Elizabeth Margaret Cunningham director**
- Phone: **+353 1 436 1000**
- Data Center: **Dublin, Ireland**

(hereinafter as: **"Google"**)

Google processes EU related data within the territory of the European Union through its servers located in Dublin, Ireland. Google may not access, modify, delete, use, or otherwise manipulate user related data stored on the server provided by Google. If, for any reason, Google processes personal data outside the European Union, it will provide adequate protection in accordance with the provisions of the GDPR. You can find more information on this here: <https://policies.google.com/privacy/frameworks>

Google provides the protection of data on multiple levels, such as physically protecting data storage servers, which are secured and supervised by security guards and technicians, it restricts access to server rooms by its employees and by providing uninterruptible power supply and other state-of-the-art infrastructure, restricting access to data, continuously monitoring its system, encryption, and firewall protection. The Google Privacy Policy is available at <https://policies.google.com/privacy>

If for any reason Google processes personal data outside the European Union, your data will still be protected by the GDPR, in light of the European Commission's adequacy decision on EU-US Data Flow Compliance Decision.

IX. What rights do You have in connection with processing Your personal data?

Request for information (right to access): You may request information about the processing of Your personal data at any time, either in person, at our registered seat address, in writing by sending a registered letter or by email to info@holospital.at

Pursuant to Article 15 Section (1) of the GDPR, a request may include information on the data processed, their source, purpose, legal ground, duration, name and address of any processor, processing activities and Your rights in relation to processing. In the case of data transfer, to whom and for what purpose Your data have been or will be transferred.

A request for information is considered authentic by us if You are clearly identified by it. If the request is sent by e-mail or post, only the e-mail sent from Your registered e-mail address will be considered as authentic, and we will only be able to send information to the postal address registered by us. Unless You voluntarily verify Your identity otherwise, we will not be able to send information to an e-mail address or postal address that is not registered in our records in order to protect Your privacy.

Rectification: You may at any time request the rectification, modification or amendment of Your data in the same manner described above. We can also do this only on the basis of a request from a credible source presented when submitting the request.

Restriction: You may request that we restrict the processing of our personal information in particular if:

- a) You argue the accuracy of the personal data we process. In this case, the limitation refers to the period during which the accuracy of the data is checked.
- b) Although the legal ground for processing does not stand for us, but You are requesting us in writing to keep them for the purpose of filing, asserting or defending any legal claim You may have

Objection If we process Your personal data on the ground of legitimate interest, You may at any time object to the processing of Your personal data. In such cases, we will review the legality of the objection and, if it is well established, we terminate the processing of data and notify anyone to whom the personal data subject to the objection may have been previously transmitted.

Deletion (“Right to be forgotten”): You may request the deletion of Your personal data at any time for any of the reasons set out in Article 17 Section (1) of the GDPR.

We may refuse deletion if the processing of Your personal data is required by law or if it is necessary to enforce our legal claims. We will always inform You about the refusal of the request for deletion. Once it is deleted, the data cannot be recovered.

Transfer of Personal Data (Portability): You may at any time request us to transfer the data processed in connection with You in a structured, widely used, machine-readable format to You or to another controller.

We kindly ask You to not exercise the above rights improperly, but only if it has a real ground or if any of the conditions set out in the GDPR actually exist.

X. To whom we transfer personal data and who has right to access them?

Your personal data will be treated confidentially and will not be disclosed to any third party, except as provided below.

X.1. Correspondence (e-mail)

For e-mail communication, the Service Provider uses the Microsoft e-mail service, the provider of which is Microsoft, detailed information about which can be found in section VIII.2.2. of this Policy.

XI. What third-party social media plug-ins may be found on our Website?

To receive feedback on the contents we share on the Website and to share them we use social media sites meaning we use the services (plugins) of third party providers. The plugins are only active when You specifically click on the button to allow them to contact social media sites. The plugins of the following two social media sites can be found on our website: X (Twitter), LinkedIn, YouTube

If You are logged in to any of these sites, it may occur that Your visit on the site will be attached to Your personal profile. If you click on the specific button, your browser will forward the relevant information directly to that social media site and store them there.

Information about the scope and purpose of the data collected, further processing of Your data and use of Your data by the social media provider, and Your rights regarding personal data can be found in privacy statements of the social media providers, which are available at:

X (Twitter): <https://twitter.com/hu/privacy>

YouTube: <https://policies.google.com/privacy>

LinkedIn: <https://www.linkedin.com/legal/privacy-policy>

XII. To whom and in what cases are we required to disclose personal data?

We are obliged to disclose the personal data we process to the competent authority upon request by such authority. We cannot be held liable for any such transfer and the consequences thereof. We will always inform You of the transfer when it becomes necessary.

XIII. What are the responsibilities with regard to the personal data You provide?

When You provide us Your personal data, You are responsible for ensuring that the information and contributions You make are true and correct.

We ask You to provide us third-party data only if specifically authorized to do so by the third party. The Service Provider assumes no liability for any resulting claims.

If a third-party objects the processing of personal data by credibly verifying its identity, we will immediately delete third-party data without notifying You. Please only provide third-party personal data only if you have informed the third party of the availability of this Policy.

Please do not provide us with any personal data in addition to the data requested by the Service Provider and specified in Chapter IV above. If you provide the Service Provider with any personal data in addition to the data requested by the Service Provider, the Service Provider will immediately render it unrecognizable and irretrievably delete it, and excludes its liability for data that the data subject has voluntarily provided to the Service Provider without the Service Provider's request.

XIV. Management of Personal data breach

Any personal data breach that may occur will be reported to the supervisory authority within 72 hours from becoming known to us in accordance with the law, and we will also maintain records of any breach that may occur. In the cases specified by law, we also inform the Data Subjects concerned.

XV. Data Protection Officer (DPO)

Pursuant to Article 37 of the GDPR appointment of a DPO is mandatory if:

- a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

With respect to that the Service Provider is not subject to any of the clauses above and because there is no other compelling reason to appoint a DPO we are not appointing anyone for this position.

XVI. Amendment of the Privacy Policy

If the scope of the data processed, the legal ground for the processing or other circumstances change, we will amend this Policy in accordance with the GDPR within 30 days and publish it on the Website and notify the Data Subject of the changes. In any case, please read the changes to this Privacy Policy carefully as they contain important information about the processing of your personal data.

XVII. Who You may contact for information regarding Your personal data or to exercise Your rights?

Please contact us with any inquiries in e-mail at info@holospital or by post at 9 Sümegvár köz, 1118 Budapest, Hungary.

The Data Subject is entitled to exercise his / her rights related to the processing of personal data against the Service Provider as controller. If You wish to exercise Your rights, You must notify the Service Provider first.

If You feel that Your rights have been violated, You can complain to the National Authority for Privacy and Freedom of Information being the competent data protection authority in relation of the Service Provider, which may be contacted at:

Name: **National Authority for Privacy and Freedom of Information**

Address: **9-11 Falk Miksa street, Budapest 1055, Hungary**

Mailing address: **1363 Budapest, PO box: 9., Hungary**

Phone: **+36 1 391 1400**

E-mail: ugyfelszolgalat@naih.hu

Website: <http://www.naih.hu>

In the event of a dispute arising out of or in connection with this the present Privacy Policy, its breach, validity or interpretation, the User may bring the dispute to the competent court under Act CXXX of 2016 on the Code of Civil Procedure (Code of Civil Procedure):

Name: **Miskolci Törvényszék (Metropolitan Court of Miskolc)**

Address: **4 Dózsa György Road, 3525 Miskolc, Hungary**

Mailing address: **3550 Miskolc PO box: 370**

Phone: **+36 46 353 411; +36 46 815-200**

E-mail: birosag@miskolcit.birosag.hu

Website: <https://miskolcitorvenyszek.birosag.hu/>