

GLOBAL SECOND OPINION GENERAL PRIVACY POLICY

Archived version: effective until 29 August 2026

GENERAL

1. The Global Second Opinion Platform ("Platform") on our website <http://www.globalsecondopinion.com/> ("Website") is provided by Medical Second Opinion Ltd. ("we", "us") whose legal representative in the EU for the purpose of data protection is Affinity Ltd. (Królowej Jadwigi 43, 61-871 Poznań, Poland - gdpr.representative@affinity-group.pl) and enables referring "Local Physicians" as well as "Patients" and "Patient Representatives" (jointly identified as "Users"), as detailed in the Terms & Conditions, to request treatment opinions ("Second Opinions") by Medical Professionals"
2. It is of utmost importance for Medical Second Opinion Ltd. ("we", "us") as a data controller with regard to data indicated in this Policy to protect your personal data. We therefore comply with the applicable data protection provisions, in particular the EU General Data Protection Regulation ("GDPR") concerning the protection, lawful processing and confidentiality of your personal data as well as data security.
3. This General Privacy Policy explains to you the nature, extent and purposes of the processing of your personal data when visiting and using our Website, which is regulated along with the related services, functions and contents as well as external web presence (together "Online Services") by:
 1. this General Privacy Policy;
 2. the Terms & Conditions;
 3. the Privacy Policy for Patients, Patient Representatives and Local Physicians; and
 4. the Cookie Policy.
4. In the following sections you will be informed which personal data we potentially collect, process and use when you use our Online Services.

WHICH OF YOUR DATA DO WE COLLECT, FOR WHICH PURPOSES, ON WHICH LEGAL BASIS DO WE PROCESS YOUR DATA AND HOW LONG DO WE STORE IT?

Contacting Us

When you fill out the contact form on our Website and send your enquiry or establish contact with us via phone call, postal mail, e-mail or through other electronic channels, we process (as a data controller) the data you voluntarily provided us with (name, e-mail address, nature of the enquiry, the subject of your message and the content of your message).

We process the data provided within the course of contacting us solely for processing your enquiry, to get in contact with you if desired and to provide you with the requested information. This data processing is therefore necessary for answering your enquiry, based on our legitimate interest, your consent, and for the fulfilment of our (pre)contractual obligations. Therefore, as soon as these purposes are completed, we erase your data.

Usage data

Based on your consent declaration, we also collect and process the following data about your use and interaction with our Website and Online Services: IP-address of your device, the used internet browser, the browser language, your operating system, the requested files from our Website, your settings regarding Java, screen resolution, color depth, your click behavior on the Website (time of access, clicks) as well as the internet site from which you visit us (referral URL).

This data is generally collected through cookies (see our Cookie Policy). We use this usage data for (i) web analysis, (ii) improvements to our Online Services and our Website and (iii) increasing usability. This data processing occurs on the basis of your consent to the use of cookies on our Website. You can withdraw this consent at any time (e.g. through your browser settings regarding cookies) with effect for the future and free of charge.

Newsletter

On the basis of your consent declaration (obtained through the double opt-in process, which means that after registering for the newsletter you receive an e-mail in which you are asked to confirm your registration), we process the personal data that you provided us with voluntarily in the course of the registration for the newsletter (your e-mail address) in order to send you e-mail newsletters about our platform, current projects, marketing and product information.

You can withdraw your consent to the receipt of our newsletter at any time (e.g. via e-mail to info@globalsecondopinion.com) or through the unsubscribe link in our e-mail newsletters) with effect for the future and free of charge. After receipt of your withdrawal, we will cease to send you e-mail newsletters and erase your personal data from the mailing list.

Provided that you have only registered for our newsletter (therefore, when you have not requested from us a second opinion from us), we store your data until the withdrawal of your consent and beyond that for a maximum of three years in order to demonstrate compliance with data protection and e-commerce regulations.

Registration and User Account

When you register on our Platform and create a user account ("Account", as defined in section 2 of the Terms & Conditions) for the use of our Online Services, we process your personal data in accordance with our Privacy Policy for Patient Representatives and Local Physicians.

Requesting and Providing Second Opinions

When you request a Second Opinion via our Website and Online Services, we process your personal data according to our Privacy Policy for Patients, Patient Representatives and Local Physicians.

Access data and log files

We collect and process the following data when you use our Website and Online Services, which means accessing the corresponding server which contains the specifically requested service (so called server log files): name of the accessed site, file, date and time of access, transmitted quantity of data, server status codes, username, processing time, browser and client type alongside the version, your operating system, referrer URL (the previously visited site), IP-address and the requesting provider, reverse DNS, location data, connection data, source and target (network discovery or address, port numbers, protocol, e-mail address, e-mail subject, connecting server, protocol details, reputation data, reverse DNS, obvious labelling, connected servers), authentication details and e-mail meta information.

This data is generated automatically through our servers when you use our services and is necessary so that we can provide you with the desired services. We therefore process server log files solely to be able to operate our Website and the connected Online Services, to identify you as a user authorized to access, to distribute web server requests in our server pool as well as for security reasons (e.g. for clarification of abusive and fraudulent activities). Thus, this data processing activity is necessary to ensure our legitimate interests in operating a user friendly and secure Website.

Without prejudice to defend our eventual liabilities as stated below, we generally store this data for 500 days since your access data and log files were collected before erasing them.

ADDITIONAL EMBEDDED SERVICES AND CONTENTS OF THIRD PARTIES

Within our Online Services, we use further services and contents of third party providers to incorporate their contents and services on the basis of our legitimate interests in the provision, optimization and economical operation of our Online Services. This regularly requires that the third parties of these contents receive the IP address of the user as they are not able to send the requested contents to the right browser without the IP address. The IP address is therefore necessary for the display of these contents and the use of the embedded services.

Specifically, we have utilized the following services and contents of third parties in our Online Services: Stripe, Google Analytics, DeepL, mailchimp and HubSpot.

IS YOUR DATA TRANSMITTED TO THIRD PARTIES?

1. We entrust your personal data to the extent necessary to the following external service providers (data processors) that support us with the performance of our services:

1. IT-service providers and/or providers of data hosting solutions or similar services;
2. Other service providers, providers of tools and software solutions, and cloud based applications that support us with the performance of our Online Services and operate on our behalf (including providers of marketing tools, communication service providers, and translators).

All our data processors process your data only on our behalf and on the basis of our instructions so that we can provide you with our Online Services.

2. Apart from this, we transmit your personal data to the extent necessary to the following recipients (controllers):
 1. External third parties on the basis of our legitimate interests in the extent necessary (e.g. auditors and tax consultants, insurances in case of insured events, legal representatives in case of incidents, courts and competent authorities, social networks);
 2. Authorities, courts and other public entities in the extent legally necessary (e.g. financial authorities);
 3. Potential third parties that are participating in the provision of services for the fulfilment of our contractual obligations (e.g. banks for processing of the payment, payment service providers);
 4. The hospitals and responsible Medical Professionals who provide the requested Second Opinion (based on the Patient's consent – given directly to us or indirectly via the other Users acting on behalf of the Patient, the Patient's vital interests and contractual relationship with a Local Physician). Hospitals and Medical Professionals are the only recipients of health data.

IS YOUR DATA TRANSFERRED OR PROCESSED OUTSIDE THE EU?

1. Yes, the hospital and/or responsible Medical Professionals, payment service providers, translators and providers of marketing tools may also be established outside of the European Economic Area (EEA), but generally we do not give them any personal data if the data subject does not contract our second medical opinion services.
2. As far as we process your data in a third country outside the European Union (EU) or the European Economic Area (EEA), this only occurs if necessary for the fulfilment of our (pre)contractual obligations, on the basis of your consent, due to a legal obligation or on the basis of our legitimate interests. We have implemented suitable and appropriate guarantees to develop a way to transmit your data to the corresponding third country compliant with data protection provisions as detailed below:

Recipient	Categories of personal data transferred	Purposes	url
Massachusetts General Hospital, Brigham & Women's Hospital, Dana Farber Cancer Institute and others (through Mass General Brigham)	Medical records, information and data, including, as the case may be, pathology specimens, radiological images, laboratory results/reports, an English translation of all relevant records, and Client consent (collectively, the "Medical Record")	Access to medical records to perform activities (provide medical second opinions)	https://poso.partners.org/Terms/PrivacyPolicy https://poso.partners.org/Terms/TermsOfUse
Boston Children's Hospital (through Summus Global)	"Medical Records"	Access to medical records to perform activities (provide medical second opinions)	https://www.summusglobal.com/Privacy
UCLA Health	"Medical records"	Access to medical records to perform activities (provide medical second opinions)	https://www.uclahealth.org/privacy-notice

HOW LONG DO WE STORE YOUR DATA?

1. We store your personal data in relation to the processing based on your consent, (pre)contractual obligations, and/or our legitimate interest, just as long as necessary for the purposes for which they are processed. Beyond that, we are potentially obligated to store your data for longer in accordance with legal retention periods.
2. Besides that, we could also store personal data beyond the above mentioned time periods as long as:
 1. Legal claims out of the relationship between users and us are possible, or until the definitive clarification of an incident or legal dispute. This longer storage occurs to ensure of our overriding legitimate interests in the enforcement, clarification and defense of our legal claims.

2. Beyond that, we are potentially obligated to store personal data for longer in accordance with legal retention periods such as the ones stated by i.e. Tort Law, Taxes, Anti-Money laundering regulation, Data Protection, Health-care liabilities, E-commerce regulations.
3. We may also store personal data blocked to deal with requests from government administrations and courts in the exercise of their functions and to defend ourselves against possible claims.
3. When you contract our services, all medical reports/records and linked personal data concerning the second opinions are stored according to our Privacy Policy for Patient Representatives and Local Physicians.

WHICH DATA PROTECTION RIGHTS DO YOU HAVE?

1. You have the right to access your personal data that is being processed by us (Art 15 GDPR). Further, you have the right to rectification of inaccurate or incomplete data and – under certain circumstances – the right to erasure (Art 16 and Art 17 GDPR). Additionally, you have the right to restriction of processing (Art 18 GDPR) as well as the right to data portability concerning the data you have provided us with (Art 20 GDPR).
2. Moreover, you have the right to object on grounds relating to your particular situation (Art 21 GDPR). Such an objection can in particular occur relating to processing of data for the purposes of direct marketing.
3. Additionally, you have the right to withdraw your consent at any time with effect for the future.
4. Finally, you have the right to lodge a complaint with the competent supervisory authority (Art 77 GDPR).
5. If you have questions relating to this or any other questions, you can contact our Data Protection Officer at: Konrad Bednarowski, Affinity Ltd., Królowej Jadwigi 43, 61-871 Poznań, Poland, gdpr.representative@affinity-group.pl

HOW DO WE SECURE YOUR DATA

1. We comply with appropriate technical and organizational security measures pursuant to Art 32 GDPR to, considering the risks, guarantee an appropriate data protection level, especially to protect the personal data against accidental or unlawful destruction, alteration or against loss and against unauthorized disclosure or unauthorized access. Our security measures include:
 1. An encrypted connection and SSL certificate.
 2. Authentication, authorization, encryption and access restriction mechanisms at the level of: firewall, server and application, firewall and antivirus protection.
 3. Security logs with digital record of server activity.
 4. The use of secure and proven solutions for database service, server website, web container, user interface and integration.

5. System design and implementation procedures based on good practices and guidelines to protect the system against the most common attacks according to the documentation of OWASP project management.
6. Forced use of secure passwords.
7. Automatic inactivity logout.
8. Secure facilities for data storage.
9. Access to information on a need-to-know basis and role-based access control.
10. Systematic anonymization or deletion of personal data, which is no longer necessary for the purposes for which were collected and processed.

AMENDMENTS TO OUR PRIVACY POLICY

We may amend this Privacy Policy from time to time in accordance with article 1.6 and 1.7. of Terms and Conditions available on our Website.