

GENERAL

1. The Global Second Opinion Platform ("Platform") under 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 Konrad Bednarowski at Affinity Ltd. (Królowej Jadwigi 43, 61-871 Poznań, Poland - gdpr.representative@affinity-group.pl) and enables referring "Local Physicians" as well as "Patients" or "Patient Representatives" (jointly identified as "Users"), as detailed in the Terms & Conditions, to request treatment opinions ("Second Opinions") by "Medical Professionals". We offer our services via the website <http://www.globalsecondopinion.com/>, which is regulated by:
 1. This Privacy Policy for Patients, Patient Representatives and Local Physicians;
 2. The General Privacy Policy;
 3. The Terms & Conditions; and
 4. The Cookie Policy.
2. It is of our utmost importance to protect any 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 (including personal data you provide to us or process for us on behalf of other people, such as Patients where you are a Patient Representative or a Local Physician) as well as data security.
3. This Privacy Policy explains to you the nature, extent and purposes of the processing of your personal data (including personal data that you provide to us or process for us on behalf of other people) when you request a Second Opinion via our Platform concerning a medical condition.
4. Through the registration process, according to section 2.1 of this Privacy Policy and our Terms & Conditions, Users create an individual profile ("Profile") with information about themselves. Further, depending on the category of User concerned, the User may perform the following actions:
 1. **Patients:** They have the possibility to upload, post and submit certain content to the Platform in order to request Second Opinions.
 2. **Patient Representatives:** When they have previously been authorized by the Patient, or in the Patient's vital interest, they have the possibility to upload, post and submit certain content to the Platform in order to request a Second Opinion on behalf of the Patient.

3. **Local Physicians:** They have the possibility to upload, post and submit certain content to the Platform in order to request a Second Opinion on behalf of the Patient (when they have been previously authorized by the Patient, or in the Patient's vital interest).
5. Where the User is a Local Physician requesting a Second Opinion, or a Patient Representative, they expressly guarantee Medical Second Opinion Ltd. that they can provide the Patient's health data for the processing intended by this Website and our Platform (including the transfer of the Patient's data including health data to the hospitals and Medical Professionals that will provide the Second Opinion) either under the "previous authorization" of the Patient or under the "vital interest" of the Patient.
6. As a consequence, where a Local Physician or Patient Representative provides us with Patient information, he/she shall be responsible to inform the Patient of the processing of his/her personal data (particularly, his/her health data) by Medical Second Opinion Ltd. by this Website and Platform. Therefore, the Local Physician or Patient Representative also guarantees that he/she obtained the appropriate prior specific authorization from the Patient to do so, unless there is one of the exceptions set out in section 2.2. of this Privacy Policy for Patients, Patient Representatives and Local Physicians and where Medical Second Opinion Ltd. is not obliged to inform the Patient.

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

Registration and User Account

1. When Users are registered on our Platform and have a user account for the use of our Online Services (an "Account" as detailed in the Terms & Conditions), we process the following personal data as data controller: title, name, date of birth, gender, country of residence, e-mail address, hospital/practice if a Local Physician creates the account, IP address, as well as your access data.
2. After completing the registration form and once the User Account has been created, a User becomes a User of Medical Second Opinion Ltd. We process the data of your User Account solely for operating your Account and the provision of our Online Services. This data processing is therefore necessary for the fulfilment of our (pre)contractual obligations.
3. We store data in connection with your registration and your User Account either until the end of your client relationship with us, or beyond that until the expiry of the respective legal retention periods (usually no longer than a time period of 7 years).

Requesting Second Opinions

1. When Users request a Second Opinion via our platform, we process the following personal data as data controller: name, date of birth, city, country, language, gender, diagnosis of the Patient, information on prior treatments and stage of

disease of the Patient, date of first diagnosis of the Patient, and reason for the Second Opinion (if applicable, the data of the Local Physician or Patient Representative).

2. In the event that Local Physicians or Patient Representatives share information about a Patient with a Medical Professional (at the hospitals providing Second Opinions) and translators (to translate the medical records) in order to obtain a Second Opinion, the Patient must have given his/her prior informed consent in accordance with article 14 GDPR given that such information cannot be completely anonymized. In case the sharing of data is necessary for the vital interests of the Patient, the User will guarantee Medical Second Opinion Ltd. to have previously informed the Patient and/or his/her legal representative of any and all processing carried out by Medical Second Opinion Ltd. through the Platform and Website, in accordance with the contracted Online Services.
3. Following the request for a Second Opinion, Medical Professionals of cooperating hospitals providing Second Opinions to the patient through our Website become independent data controllers upon data transfer and will draft and share the requested Second Opinion so that the requester can access it. In this case, we process the following details of the Second Opinion: name and location of the Patient (if applicable, name and location of the Local Physician or Patient Representative), date of the Second Opinion request, date the Second Opinion was completed, hospital which completed the consult, and modifications of the diagnosis/treatment/management based on the Second Opinion.
4. The data processing is necessary for the fulfilment of our (pre)contractual obligations. Further, the processing of special categories of personal data (e.g. health data) is based on the same legal basis as mentioned in the second paragraph of section 2.2 above.

WHERE DO WE RECEIVE THE PERSONAL DATA FROM?

1. Depending on who requests the Second Opinion, we receive the personal data either directly from you (or if applicable, from the Patient Representative or Local Physicians). Further, the data within the Second Opinion results from cooperating hospitals/physicians in the USA.

IS THE PERSONAL DATA TRANSMITTED TO THIRD PARTIES?

1. We entrust your personal data (if applicable, also the personal data you provide us with from other persons) only to the extent necessary to the following external service providers (data processors) that support us with the performance of our services:
 1. Translators;
 2. IT-service providers and/or providers of data hosting solutions or similar services;

3. 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 and communication service providers).

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

1. Apart from that, we transmit the personal data in the extent necessary to the following recipients:
 1. 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);
 2. 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);
 3. External third parties based on our legitimate interests only to 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);
 4. Authorities, courts and other public entities to the extent legally necessary (e.g. financial authorities).

IS THE PERSONAL DATA TRANSFERRED OR PROCESSED OUTSIDE THE EU

1. Yes, the hospitals and/or responsible Medical Professionals, payment service providers, translators and providers of marketing tools are located in the United States.
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 of transmission of your data to the 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 THE PERSONAL DATA?

1. We store the User's personal data just as long as necessary for the purposes for which they are processed and according to legal obligations except if or when User's and/or Patient's consent is withdrawn. Nonetheless, we may carry on with the processing of personal data if we have another legal basis to do it, for example when the processing is needed for the vital interests of the Patient or because of the contractual relationship with a Local Physician subject to the obligation of professional secrecy under Union or Member State law. In any case, we can store and process health data for archiving purposes in the public interest, scientific research, statistical or other purposes, and if we do so, the health data shall be anonymized so that the person concerned cannot be identified.
2. Besides the above, we could also store the personal data beyond the above mentioned time periods as long as:

1. Legal claims resulting from 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 our overriding legitimate interests in the enforcement, clarification and defense of our legal claims.
2. In addition, we are potentially obligated to store the personal data for longer in accordance with legal retention periods such as the ones stated i.e. by Tort Law, Taxes, Anti-Money laundering regulation, Data Protection, Health-care liabilities, or E-commerce regulations.
3. We may also store personal data to address requests from government administrations and courts in the exercise of their functions and to defend ourselves against possible claims.

WHICH DATA PROTECTION RIGHTS DO USERS HAVE?

1. Users have the right to access their personal data that is being processed by us (Art 15 GDPR). Further, they 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, they have the right to restriction of processing (Art 18 GDPR) as well as the right to data portability concerning the data they have provided us with (Art 20 GDPR).
2. Moreover, Users have the right to object on grounds relating to their 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, Users have the right to withdraw their consent at any time.
4. Finally, Users have the right to lodge a complaint with the competent supervisory authority (Art 77 GDPR).
5. If Users have questions relating to this or any other questions, they can contact our Data Protection Officer at: Affinity Ltd., Królowej Jadwigi 43, 61-871 Poznań, Poland, Electronic address: gdpr.representative@affinity-group.pl

HOW DO WE SECURE THE PERSONAL DATA?

1. We comply with appropriate technical and organizational security measures pursuant to Art 32 GDPR, considering the risks, to 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. 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 they were collected and processed.

AMENDMENTS TO OUR PRIVACY POLICY FOR PATIENTS, PATIENT REPRESENTATIVES AND LOCAL PHYSICIANS

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.