Sikos Plastic Surgery, Hair Transplant Clinic

Privacy Policy – Data Protection Guide

1. Preamble

1. The operator of Sikos Plastic Surgery, Hair Transplant Clinic (hereinafter referred to as Clinic) as Data Controller hereby draws the attention of its all patients, as well as visitors (hereinafter referred to collectively as Data Subject(s)) of the website that if you want to be the user of the website above, or wishes to be the customer of the Data Controller, then carefully read the concerning contract and the present Data Protection Guide (DPG).

2. Sikos Plastic Surgery, Hair Transplant Clinic is dedicated to protecting the privacy of the Data Subject. This Data Protection Guide explains the Data Controllers' policies and practices regarding the personal information it manages.

2. Definitions

1. Data Subject: any specific natural person identified or identifiable (directly or indirectly) based on the personal data, primarily Data Subject is the patient of the Clinic.

2. Data Controller: the natural or legal persons or organizations not having a legal personality, who or which determine the purpose of data management on its own or together with others, and make and carry out the decision regarding data management (including the equipment used), or have the data processor entrusted by them to carry out such decisions; Data Controller is determined in the chapter 3.

3. Clinic means the Sikos Plastic Surgery, Hair Transplant Clinic operated by the Data Controller.

4. Personal data: any data that can relate to the Data Subject - especially the Data Subject's name, identification number, as well as one or more pieces of information characteristic of their physical, physiological, mental, economical, cultural or social attributes - and any such conclusions regarding the Data Subject that can be drawn from such data;

5. Consent: voluntary and specific expression of the Data Subject's intention, which is based on proper information and by which the Data

Subjects provide a clear and unambiguous consent to managing their personal data comprehensively or for particular operations;

6. Objection: a statement by the Data Subjects in which they object to the management of their personal data and request the termination of data management and/or the deletion of the data managed;

7. Data management: regardless of the procedure applied; any operation or the whole of operations performed on data, specifically including the collection, recording, systematization, storage, modification, application, query, transfer, publication, harmonisation or linking, blockage, deletion and destruction of data, as well as the prevention of the further usage of such data, photographing, audio or visual recording, as well as the recording of physical attributes suitable for the identification of a person (e.g.: finger- or palm prints, DNA samples, iris scans);

8. Data transfer: rendering data accessible for certain third parties;

9. Publication: rendering data accessible for the general public;

10. Data deletion: rendering data unrecognisable in such a manner that their restoration is no longer possible;

11. Tagging data: applying an identifying mark to the data in order to distinguish them;

12. Data blocking: applying an identifying mark to the data in order to block their management for a defined period of time or for good;

13. Data processing: performing any technical tasks related to data management operations, regardless of the method and equipment applied for the performance of such operations as well as of the place of application, provided that the tasks are performed in terms of data;

14. Data processor: natural or legal persons and/or organizations not having a legal personality, who or which perform data processing activities based on their contract with the Data Controller - including contracts concluded pursuant to legal provisions;

15. Third party: natural or legal persons and/or organizations without a legal personality, who or which are not identical with the Data Subject, the Data Controller or the data processor.

16. DPG means the present Data Protection Guide, available on the website and on the front office desk of the Clinic.

3. Data Controller

1. According to the present Data Protection Guide, the Data Controller is:
    a) Síkos Orvosegészségügyi Kft.
        i. Site: 1113 Budapest, Edömér utca 6. 3/3.
        ii. Address of the Sikos Plastic Surgery, Hair Transplant Clinic: 1113 Budapest, Edömér utca 6. 3/3.
        iii. Company reg. number: 01-09-260719
        iv. Tax nr: 10808098-1-43
        v. Phone: (06-1)-209-2930 and 0620-373-3087
        vi. E-mail: info@sikos.hu
        vii. General manager: Mr. Géza Sikos M.D.
        viii. Websites: www.sikos.hu and www.shklinika.hu
        ix. Social networking website: https://www.facebook.com/SikosKlinika/?fref=ts

    b) every employee of the Síkos Orvosegészségügyi Kft.

4. The aim of the Data Protection Guide

1. The Data Controller respects the personal rights of the Data Subject, hence it prepared this DPG which is available in electronic format at the Data Controller's website as well as in print format in the Clinic.

2. Therefore the aim of the DPG is to regulate the data management procedures, methods to protect the privacy of the Data Subjects.

3. The Data Controller hereby states that it observes the provisions of
    a) the Regulation (EU) 2016/679 of the European Parliament and of the Council,
    b) the Act 112 of 2011 (hereinafter: "Data Protection Act") on the rights for information management and freedom of information,

c) the Act 154 of 1997,
d) the Act 47 of 1997,
e) the Act 133 of 2005 and
f) other Hungarian acts and rules.

5. The scope of the DPG

1. The DPG applies for all data managements in the Clinic executed by the Data Controller.

2. According to the section 1, the present DPG regulates the methods of the data managements.

3. The personal scope of the DPG is the Data Controller and the Data Subject.

4. The present DPG valid from 1st February, 2017.

6. Rights

1. Data Subjects have rights related to the data and data management.

2. Data Subjects may enforce their rights by sending request(s) to the Data Controller's postal (1113 Budapest, Edömér utca 6. 3/3.) or e-mail address (info@sikos.hu), by phone, or personally, or any available contact form.

3. Upon requests, the Data Controller shall immediately take the necessary steps based on the request and inform the Data Subjects about the taken steps within 15 days.

a) Right to information

1. Upon requests sent by the Data Subjects, the Data Controller shall provide information regarding the particular subject's data managed by the Data Controller; the source of such data; the purpose, legal basis and duration of the data management; the names and addresses of data processors as well as their activities related to data management; and (in the case of a transfer of the Data Subject's

personal data) the legal basis and recipient of data transfer. Such information shall be provided within 15 days, free of charge.

2. If the provision of information is denied, the Data Controller shall inform the Data Subject in writing as to which provision of which law was the legal basis to deny the information, and also inform the Data Subject regarding options for legal remedy.

b) Corrections

1. If the personal data are incorrect, and the correct data are available to the Data Controller, it shall correct such personal data.

2. The Data Controller shall inform the Data Subject regarding the correction as well as all parties that may potentially have received the data from the Data Controller for data management purposes. Such notice is omissible if the rightful interest of the Data Subject is not violated in terms of the purpose of data management.

3. Corrections upon request, deadline for administration and legal remedy are governed by the present DPG.

c) Right to erasure

1. The Data Subject shall have the right to obtain from the Data Controller the erasure of personal data concerning him or her without undue delay.

2. Where the Data Controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the Data Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the Data Subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

d) Right to restriction of processing

1. The Data Subject shall have the right to obtain from the Data Controller restriction of data processing.

e) Right to data portability

1. The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Data Controller without hindrance from the controller to which the personal data have been provided, where:
   a) the processing is based on consent/contract pursuant and
   b) the processing is carried out by automated means.

f) Right to object

1. The Data Subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling.

g) Automated individual decision-making, including profiling

1. The Data Subject shall have the right 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.

2. Data Subject has the right to request the deletion or blocking of the personal data, or object against the data managements.

3. Cases of deletion and blocking of personal data and objections against data management are governed by the relevant provisions of the Data Protection Act in Sections 17 - 21.

4. The Data Controller shall provide information on the legal regulations laid out in this paragraph upon requests sent to

4. Remedy

1. If their privacy rights are probably breached or breached, Data Subjects may request an investigation from the Hungarian National Authority for Data Protection and Freedom of Information. The contact details:
    a) H-1125 Budapest, Szilágyi Erzsébet fasor 22/C.
    b) Phone: +36 -1-391-1400
    c) Fax: +36-1-391-1410
    d) E-mail: privacy@naih.hu

2. If their privacy rights are breached, Data Subjects may file a lawsuit against the Data Controller. The court procedure shall be governed by provisions in Section 22 of the Data Protection Act, and the First Book, Chapter Three, Title XII (Sections 2:51 - 2:54) of Act V of 2013 concerning the Civil Code, and other relevant legal provisions.

3. The Data Controller shall provide information on the legal regulations laid out in this paragraph upon requests sent to info@sikos.hu

5. Compensation and injury claims

1. If the Data Controller causes injury or violates the Data Subject's privacy rights through handling the Data Subject's data in an unlawful manner or through violating its data security requirements, then the affected party may demand an injury claim from the Data Controller.

2. The Data Controller shall be exempt from liability for the damage caused and from its obligation to compensate an injury claim, if it can prove that the damage or violation of the privacy rights of the affected party was caused by an unavoidable force falling outside the scope of data management.

3. The Data Controller shall be exempted from liability and its obligation to compensate an injury claim, if it can prove that the damage or violation of the privacy rights of the affected party was caused by an unavoidable force outside the scope of data management. The damage may not be compensated and an injury claim may not be demanded, if it was due to the willful or grossly negligent misconduct of the damaged party.

6. Principles

1. Personal data shall be:
    a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject ('lawfulness, fairness and transparency');
    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 ('purpose limitation');
    c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
    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 ('accuracy');
    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 ('storage limitation');
    f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The Data Controller shall be responsible for, and be able to demonstrate compliance with section 1 ('accountability').

7. Legal basis

1. The legal basis of the personal data management is:
    a) the consent of the Data Subject or

b) compulsory requirement by (the Hungarian or EU) law

2. Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the Data Subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means.

3. Data Subject shall expressly consent to this DPG by
   a) accepting the DPG or
   b) using the services of the website or of the Data Controller.

4. If the management or processing of personal data based on mandatory by law, then the relevant rules are determining the purpose, the period of time, the handled data, the rights and obligations.

4. The Data Controller shall only manage personal data for pre-determined purposes, for the necessary period of time and in order to exercise its rights and fulfill obligations. The Data Controller shall only manage such personal data that are indispensable and suitable for fulfilling the objective of the particular data management activity.

5. If the Data Controller uses the received data for any other purpose than the original purpose of data collection, the Data Controller shall inform the Data Subjects in each case and ask for their specific, prior consent and/or shall provide an opportunity for them to disallow such usage.

6. Personal data communicated to the Data Controller during the data management process shall only be disclosed to such persons contracted or employed by the Data Controller entrusted with duties in relation to the given data management process.

8. <u>The period of data management</u>

1. Data Controller shall manage the data until
   a) the purpose of the data management is fulfilled;
   b) the withdrawal of the voluntary consent;
   c) statutory deadline expired; and
   d) erasing the personal data.

9. Data management – *Request for information*

1. In the case of information request, the Data Controller requests/may request that the Patient makes the following data available:
    a) name
    b) phone number
    c) e-mail address
    d) question

2. Purpose of the data management: to provide relevant information to the Data Subject.

3. Period of data management: the purpose of the data management is fulfilled.

10. Data management – *Request for quotation*

1. In the case of quotation request, the Data Controller requests/may request that the Data Subject makes the following data available:
    a) name
    b) phone number
    c) e-mail address
    d) callback request
    e) details of requested service(s)

2. Purpose of the data management: to provide relevant quotation to the Data Subject.

3. Period of data management: the purpose of the data management is fulfilled.

11. Data management – *Book an appointment*

1. In the event that Data Subject books an appointment to use a service provided by the Data Controller, the Data controller requests/may request that the Data Subject makes the following data available:

    a) name

    b) phone number

c) e-mail address

d) time

e) the booked service

2. Purpose of the data management: to provide the booked service on time to the Data Subjects, and to contact Data Subjects.

3. Period of data management: the withdrawal of the voluntary consent; the purpose of the data management is fulfilled.

12. Data management – *Management of health data*

1. If the Data Subject would like take part in health services provided by the Data Controller, then the Data Subject can make the following data available:
   a) name
   b) phone number
   c) e-mail address
   d) health data

2. Purpose of the data management: to provide appropriate health services and contact Data Subject.

3. The Data Controller (therefore every employee of the Data Controller) is obliged to manage the health data in strict confidence, according to the Hungarian law (Act 47 of 1997).

4. The health data can not be transferred to another Data Controller, and/or can not be known by other employee without written prior consent of the Data Subject.

5. Period of data management: the health data and health documentation shall be mandatorily stored by the Data Controller at least 30 years, final reports shall be stored at least 50 years according to the Act 47 of 1997.

13. Data management – *Medical agreements*

1. In the event that Data Subject and Data Controllers enter into a medical agreement, the Data Controller requests that the Data Subject makes the following data available:
    a) name
    b) mother's name
    c) birth of place and data
    d) postal address
    e) phone number
    f) e-mail address
    g) health data

2. Purpose of the data management: to provide appropriate health services according to the agreement and contact Data Subject.

3. The rules of the health data management shall be applied on the data management of medical agreement.

14. Data management – *Discounts for Patients*

1. If the Data Controller would like to give special discounts for the Data Subject, the Data Controller may request that the Patient makes the following data available, and Data Controller has to manage these data separately from other data:
    a) name
    b) provided service(s)
    c) discount
    d) phone number
    e) e-mail address
    f) health data

2. Purpose of the data management: to provide discounts for Data Subject and contact Data Subject.

3. The rules of the health data management shall be applied on the data management of discounts.

15. Data management – *Patient questionnaire, evaluation system and handling complaints*

1. As part of the quality assurance process applied by the Data Controller, Data Subjects may provide feedback on the (health) services via an online or paper-based Patient questionnaire and/or evaluation system.

2. When filling out the questionnaire, Data Subjects may provide the following personal data:
    a) name;
    b) date(s) of provided (health) service(s) and service(s);
    c) multistage evaluation
    d) note

3. Providing these data are not obligatory, and merely serve the purpose of an accurate investigation of possible complaints and/or enable the Data Controller to respond to the Data Subject.

4. The feedback received in this manner and the data potentially provided by the Data Subject may not be traced back to the Data Subject or linked to the name of the Data Subject, but may be used by the Data Controller for statistical purposes.

5. In the event that Data Subject has complaint, the Data Controller has to investigate and answer it in 30 days. In this case, the data management is mandatory, the Data Controller is obliged to manage the data, the complaint and the answer in 5 years, according to the Act 155 of 1997.

6. Period of data management: the purpose of the data management is fulfilled, or in the case of mandatory data management is 5 years.

16. Data management – *Newsletter*

1. In the case of newsletter, the Data Controller may request that the Data Subject makes the following data available:

a) name
b) e-mail address

2. Newsletter is sent by email to those who explicitly request it.

3. The provision of personal data is facultative. The eventual refusal to provide such data will make it impossible to utilize the newsletter service.

4. Data Subject can unsubscribe from the newsletter by clicking on the unsubscribe link on the end of the newsletter, or by sending request to the Data Controller's postal (1113 Budapest, Edömér utca 6. 3/3.) address.

5. Period of data management: the withdrawal of the voluntary consent.

17. Data management – Banking data

1. If the Data Subject transfers the payable amount to the Data Controller, then the following data shall be available for the Data Controller:
   a) account holder's name;
   b) account number;
   c) message;
   d) amount

2. The Data Controller is obliged to manage the data in strict confidence, according to the Hungarian law.

3. Period of data management: the withdrawal of the voluntary consent; the purpose of the data management is fulfilled.

18. Data management – *Social media*

1. The Data Controller can also be contacted via social networking site.

2. The purpose of data management is to share the contents of the website. Data Subjects may request information, quotation, etc via the social networking sites.

3. By following the Data Controller's page, the Data Subjects consent to the Data Controller posting its news and offers on the Data Subjects' news wall.

4. You can find further information about the data management in the data protection guidelines and rules of the relevant social networking page.

19. Data management – *Publication of the digital records about the Data Subject*

1. With the prior written consent of the Data Subject, the Data Controller shall record digital pictures, videos, audio materials and others (hereinafter collectively referred to as records) about the Data Subject, the provided service(s), the results and publish the records on the Data Controller's website and/or social media sites.

2. The Data Subject may be identified or identifiable (directly or indirectly) based on the records, the managed data:
   a) name
   b) record(s)
   c) date of the record(s)

3. Purpose of the data management: to promote the Data Controller's services and contact Data Subject.

4. Period of data management: the withdrawal of the voluntary consent.

20. Data management – *Surveillance cameras*

1. The Data Controller operates surveillance cameras in the area of the Clinic in order to ensure the security of Data Subjects and their property. Camera surveillance is indicated by a pictogram and a warning sign with text.

2. The purpose of camera surveillance is the protection of property. More specifically, the purpose is to protect equipment with significant value as well as the personal valuables of Data Subjects regarding detecting breaches of the law and catching perpetrators in the act, and the

prevention of such criminal acts cannot be done in any other way, and/or there is no other method of presenting evidence.

3. The floor map and the locations of the cameras marked on it are available on the front office desk of the Clinic.

4. Period of data management: 3 working days after recording in the absence of use according to the Act 133 of 2005.

21. Data management – *Website traffic data*

1. References and link: The Data Controller's website may contain links that are not operated by the Data Controller, and are only there to inform visitors. The Data Controller has no influence whatsoever on the content and security of the websites operated by partner companies, and therefore it is not responsible for them either. Before providing your data in any form at the given site, please review the data protection statements and data management guidelines of the websites you visit.

2. Analytics, cookies: In order to monitor its websites, the Data Controller uses an analytical tool which prepares a data string and tracks how the visitors use the Internet pages. When a page is viewed, the system generates a cookie in order to record the information related to the visit (pages visited, time spent on our pages, browsing data, exits, etc) but these data cannot be linked to the visitor's person. This tool is instrumental in improving the ergonomic design of the website, creating a user-friendly website and enhancing the online experience for visitors. The Data Controller does not use the analytical systems to collect personal information. Most Internet browsers accept cookies, but visitors have the option of deleting or automatically rejecting them. Since all browsers are different, visitors can set their cookie preferences individually with the help of the browser toolbar. You might not be able to use certain features on our website if you decide not to accept cookies.

22. Data safety

1. The Data Controller takes all the measures that can be expected from it for the safety of the stored data, it provides for their guarding at an appropriate level with particular regard to unauthorized access,

alteration, forwarding, disclosing, cancellation of destruction as well as to accidental destruction and damaging.

2. The Data Controller provides for appropriate technical and organizational measures in order to maintain safety of the stored data.

23. Data management – *Data processor*

1. The Data processors are determined and named in the Annex 1.

24. Data transfer

1. The Data Controller has the right to transfer personal data handed over to business partners (compliance assistants) fulfilling the Data Controller's obligation related to the Data Subjects. Such data transfer may only take place if the Data Subjects have been informed in advance accordingly, upon using the service(s) and the consents have been given by the Data Subjects.

2. The Data Controller may transfer the following data to its compliance assistants regarding to the previous section:
    a) name

3. In order to verify the legality of data transfer and inform the Data Subjects, the Data Controller shall keep a data transfer log containing the time of transfer of the managed personal data, the legal basis and addressee of data transfer as well as the definition of the scope of the transferred personal data, and any data defined in the rule of law prescribing data management.

25. Medical confidentiality

1. According to the Act 154 of 1997, article 138, Data Controller and its all employees shall keep the Data Subject's (as patient's) personal health data private, unless
    a) consent to release the information is provided by the Data Subject, or
    b) the disclosure of the health data is an obligation by law.

26. Miscellaneous rules, governing law, jurisdiction

1. The applicable version of the DPG is continuously available on the website and on the front office desk of the Clinic.

2. The legal relationship between the Data Controller and the Data Subject, and the data management shall be governed by the Hungarian law.

Closed: 1st February, 2017

Síkos Orvosegészségügyi Kft.
Mr. Géza Sikos M.D.
Managing Director