INFORMATION OBLIGATION GDPR 13.06.2020
Dr Osuch Clinic

In accordance with the binding laws regarding protection of personal data, in particular European Parliament and Council Regulation 2016/679 of 27 April 2016 regarding protection of physical persons with reference to processing personal data and on the free movement of such data, and repealing Directive 95/46/WE (GDPR) as well as The Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws 2018, item 100) to ensure proper protection of the personal data of a subject, one needs to first and foremost provide the information regarding the processing of subject's data stated in GDPR article 13 or 14 — depending on whether they were gained directly from the person they refer to, or any other source.

In light of the above, we provide the following information regarding the processing of personal data.

Information regarding the processing of personal data

1. Personal Data Administrator

The administrator of your personal data is Piotr Osuch Chirurgia Plastyczna, address: ul. Puławska 488 in Warsaw 02-884, NIP: 5212843906, REGON: 016043400, hereinafter referred to as "the Data Administrator" or "the Practice".

2. Contact date of Personal Data Administrator and Personal Data Inspector

The Personal Data Administrator may be contacted by email recepcja@drosuch.pl, by traditional post, address: Dr Osuch Clinic (Piotr Osuch Chirurgia Plastyczna), ul. Puławska 488, Warszawa 02-884, electronically: recepcja@drosuch.pl, via contact form on the website https://www.drosuch.com/contact/or by phone: +48 501 093 653. The Data Administrator has appointed a Personal Data Inspector: Elzbieta Plichta-Osuch, who may be contacted electronically: recepcja@drosuch.pl.

3. The source of data – where the data is obtained from?

a. Your personal data may be processed on the basis of GDPR article 6 section 1 point a, i.e. on the basis of the consent for processing your personal data expressed voluntarily at the time of the sending a request:
   - via contact form on the website https://www.drosuch.com/ or www.drosuch.pl in order to process message you sent,
   - in person,
   - via online or traditional (in person) registration system,
   - by subscribing to the newsletter
   - by phone.

b. Personal data given by you might be processed on the basis of GDPR article 6 section 1 point b — i.e., processing is necessary for the performance of the contract (provision of medical or other services including commercial services) to which you are a party or the undertaking of activities on your demand before the conclusion of the contract. In justified cases, data might also be obtained from other medical facilities, laboratories, etc. Your personal data might be obtained from close persons in extraordinary situations when the condition of your health requires it.

The scope of the processing of personal data

1. Scheduling a consultation requires processing of your data including the following information: name, surname, age, phone number, and email address. When registering for a consultation at the Clinic, you personally give your gender, Personal Identification Number (PESEL) or the date of you birth/ passport number (in the absence of a PESEL), as well as your place of residence. Before a surgical treatment, you also personally provide the telephone number of a close person who should be notified in emergency situation connected with deterioration of your health.

2. This data is also used to verify your identity before the provision of a service. Your personal data given to the receptionist/ medical staff in the headquarters of the Data Administrator are processed on the basis of GDPR article 9 section 2 point a – in order for the Data Administrator to undertake activities connected with the provision of medical services.

3. Upon conclusion of the agreement with the Data Administrator as to the provision of medical services, the legal basis for processing your personal data is GDPR article 9 section 2 point h, and the data is processed for the purpose of the

proper fulfilment of the contract, including the appropriate conduct of plastic surgery consultation and/or procedure as well as providing health services connected with the procedure (hospitalization, preventive maintenance) carried out by the Data Administrator.

4. Furthermore, the Data Administrator remains obliged by law, including by The Act of 6 November 2008 on Patients' Right and the Ombudsman for Patients' Rights, to archive medical documentation generally for a period of 20 years from the end of the calendar year in which the last entry was made. Data included in medical documentation include among others the following: description of your treatment process, the diagnosis, and recovery. If you expressed consent for marketing communication, data in the form of your email address, name, and surname are used.

Purposes of processing of personal data and legal basis for processing

1. The provision of health services (e.g., diagnosis, preventive maintenance, and therapy) as well as management process (e.g., financial issues regarding payments for services, preparing medical documentation, and verification of identity prior to your treatment):

    - The legal basis: GDPR article 9 section 2 point h in connection with provisions regulating the process of the provision of health services, specifically provisions of The Act of 15 April 2011 on Medical Activity, and The Act of 6 November 2008 on Patients' Rights and the Ombudsman for Patients' Rights.

2. Keeping accounting records and tax settlements:

    - The legal basis: GDPR article 6 section 1 point c in connection with the provisions of The Act of 29 September 1994 on Accounting and The Act of 11 March 2004 on the Tax on Goods and Services.

3. Your personal data might be processed in order to protect rights and pursue claims by the Data Administrator in connection with the activity run by him.

    - The legal basis: GDPR article 6 section 1 point b and f and in the case of sensitive data GDPR article 9 section 2 point f.

4. If you gave consent for marketing communication, your data might be used in order to inform you about products and services offered by the Administrator as well as eduction/ information in the form of blog articles:

    - The legal basis for the data processing is your consent in accordance with GDPR article 6 section 1 point a.

Data retention period

1. In accordance with the requirement of the provision article 29 of The Act of Law of 6 November 2008 on the Rights of the Patient and the Ombudsman for Patients' Rights, your personal data included in the medical documentation of the Practice will be retained for a period of 20 years extending from the end of the calendar year in which the last entry was made, with the exception of:

    - medical documentation in the case of the death of a patient as a result of bodily harm or intoxication is to be retained for a period of 30 years extending from the end of the calendar year in which the death occurred;
    - medical documentation comprising data necessary to monitor the fate of blood and its components for a period of 30 years extending from the end of the calendar day in which the last entry was made;
    - X-ray images retained outside the patient's medical documentation, which are to be retained for a period of 10 years extending from the end of the calendar year in which the image was taken;
    - referrals for tests or doctor's recommendations, which are retained for a period of:

        - 5 years extending from the end of the calendar year in which the health service was provided, which was the subject of a referral or a doctor's order;
        - 2 years extending from the end of the calendar year in which a referral was issued but a health service was not provided because of the patient's failure to appear at the agreed date, unless the patient collected the referral;
        - medical documentation regarding children until the age of two, which is to be retained for a period of 22 years.

2. After the expiration of the periods indicated in section 1, the subject providing the health services will destroy the medical documentation in a manner so as to prevent the identification of the patient it referred to, or it may be handed

over to the patient, to their statutory representative, or to a person authorized by the patient. Personal data that could be used for protecting rights or pursuing claims will be processed until the expiry of these claims according to the provisions of The Act of 23 April 1964 Civil Code.

3. Personal data processed for the purpose of bookkeeping and accounting and fulfilling public-law obligations including tax obligations will be processed until the expiry dates of public-law obligations — i.e., generally for a period of 5 years from the end of the calendar year in which the tax obligation was established. Additionally, personal data might be retained by the Data Administrator for the purpose of preventing malpractice or fraud, or for statistical and archival purposes for the period of 10 years from the day of termination of the agreement or an event causing the necessity of such processing.

4. Your personal data processed by the Data Administrator on the basis of an expressed consent for contact for marketing purposes will be processed for a period of 10 years or until the time of withdrawal of consent for their processing.

Recipient of data

1. The Personal Data Administrator states that your personal data might be disclosed to third parties if such an obligation arises from legal provisions — e.g., pursuant to the provision of article 26 of The Act on Patients' Rights and the Ombudsman for Patients' Rights — including persons authorized by the patient, subjects delivering health services in order to provide continuity of health services as well as public authorities including the Ombudsman for Patients' Rights, self-governing bodies of medical professions as well as national and regional consultants to the extent necessary for those bodies to perform their tasks, specifically supervision and control.

2. Personal data might also be entrusted to third parties on the basis of a personal data processing agreement solely in line with the Data Administrator's orders if it is necessary for the realization of data processing purposes or provision of the Data Administrator's services including, among others, IT service providers (such as Zenbox.pl/ hekko.pl, Get Response), entities providing accounting-bookkeeping services, and marketing agencies (on condition that you expressed consent for contact for marketing purposes).

Transfer of personal data beyond the European Economic Area (EEA)

1. The Data Administrator uses the services and technologies offered by Facebook Inc. such as: Facebook, Messenger, WhatsApp and Instagram, and YouTube.

2. The Data Administrator states that Facebook Inc., YouTube is based outside the European Union, and therefore in the light of the provisions of the GDPR is treated as an entity operating on the territory of a third country.

3. The Data Administrator ensures that when using services and technologies, he transfers personal data only to entities from the United States and only those that have joined the Privacy Shield program on the basis of a decision Executive Committee of the European Commission of July 12, 2016 - more on this topic can be read on the website European Commission available here:
https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_pl.

4. Detailed information on the transfer of data outside the EEA has been regulated in the privacy policy.

The rights of the data subject

1. In connection with the processing of your personal data, you have the right to:

   a. Access your personal data,
   b. Correct your personal data,
   c. Delete your personal data on condition that this is possible pursuant to the provisions of GDPR article 17 — for example, personal data is not necessary for the purposes for which they were collected or they were processed in a different way, or the person withdrew consent on the basis of which the Data Administrator processed personal data and there is no other basis for legal processing of personal data. The right to delete data might be restricted because of overriding duties of the Data Administrator including medical record keeping.
   d. Demand that the Data Administrator restrict your personal data processing. The right to restrict data processing might be limited because of overriding duties of the Data Administrator including medical record keeping.
   e. Lodge an objection against your personal data processing, transfering your data,

f. Lodge a complaint about personal data processing in cases specified in GDPR article 21 to the supervising body in charge of personal data protection (i.e., the President of the Personal Data Protection Office, ul. Stawki 2, 00-913 Warszawa).

2. One may exercise the above rights, specifying the content of the demand:
   a. By email: recepcja@drosuch.pl
   b. By traditional post at the address: Piotr Osuch Chirurgia Plastyczna, ul. Puławska 488, Warszawa 02-884.

Information on freedom to disclose data

1. Disclosing personal data is a necessary prerequisite for the provision of health services due to legal requirements imposed on the Data Administrator including the necessity to keep medical records. Refusal to disclose personal data is a basis for the refusal to provide health services. Disclosing data is also necessary for the issuance of the bill or invoice.
2. Disclosing personal data for marketing purposes is voluntary. The lack of consent for marketing communication is not a basis for the refusal to provide health services.

Information on automated decision-making

1. Your personal data may be processed in an automated manner and be subject to profiling (e.g. in as part of automated feedback or as a result of marketing goals through evaluation of some of your personal factors).

2. The processing of personal data in an automated manner and their profiling is primarily aimed at improving the provision of services by the Administrator, adapting goods or services to your needs, or increasing your satisfaction.