No. Phone: 11.17.001.007.062 September 6, 2019 XXXXXXXXXXXXXXX Doctor and Director of the company XXXXXXXXXXXX, BY THE COMMISSIONER FOR PERSONAL DATA PROTECTION DECISION SUBJECT: Complaint for violation of the GDPR 1. Facts: 1.1. On 31/5/2019 XXXXXXXXXXXX (hereinafter “Complainant”) submitted a complaint to the Office of the Commissioner for Personal Data Protection regarding the processing of her personal data from the official profile of the practice, @XXXXXXXXXXX, on a Social Networking Media, namely Instagram. 1.2. Specifically, the Complainant's allegations related to the following: 1.2.1. The Complainant on 8/30/2017 underwent a rhinoplasty operation by you, XXXXXXXXXXXX, (hereinafter "Complainant"). The Complainant considers that the operation is a very personal event and that the publication of the said video and photos showing the before and after the operation, concerns sensitive personal data. In addition, the publication and/or communication and/or disclosure of the material in question was done without the face being altered or at least covered in a way that the Complainant is not recognized and this fact has angered her, hurt her and violated her right not to it became widely known that she had undergone a rhinoplasty operation. 1.2.2. You asked the Complainant to videotape herself on your personal phone both before and after the rhinoplasty. 1.2.3. On 5/22/2019, a friend of the Complainant found that on the official profile of the clinic on Instagram (@XXXXXXX) the before and after rhinoplasty was published as an advertising spot, without any change in the Complainant's facial features, The the same spot was also published on Instagram TV (IGTV). The Complainant provided us with a copy of the relevant video. 1.2.4. As soon as the Complainant was informed of the publication and/or posting and/or sharing of the specific advertising video, she sent a personal message to the official profile of your practice (XXXXXXXXXXXXXXX) on Messenger requesting the immediate removal of the specific video from Instagram, stating among other things that she never gave her consent for the publication of the said video or other photos of her. The head of the clinic's marketing department responded to the said request of the Complainant and said that she apologizes on your behalf for the misunderstanding. The message also stated that the video in question was mistakenly sent by the Clinic to be used by the Marketing Department. Both the video and the Complainant's photos were removed from all pages of the Clinic. He apologized again and told the Complainant that he could contact her on her personal phone. 1.3. Pursuant to Article 57(1)(f) of Regulation (EU) 2016/679 (hereinafter "GDPR 2016/679"), on 10/06/2019 via e-mail my Office informed you about the allegations of the Complainant and asked for your own opinions and positions on the matter. 1.4. In an electronic message dated 4/7/2019 sent by XXXXXXXXXXXXXX on your behalf, your letter dated 3/7/2019 was attached, in which the following are mentioned: a) the Complainant underwent surgery by you on

30/8/2017, b ) gave relevant consent for the use of photographic and video material taken during the operation for promotion and/or advertising purposes of your Clinic, c) the video recording was made by the Complainant herself using your personal phone, d) snapshots from the operation were published on 22/5/2019 in Social Media, namely on Instagram, on the official profile of the clinic @XXXXXXXXX. e) the Complainant in a personal message on messenger requested the removal of the relevant material posted and at her request, all photographic and/or video material was IMMEDIATELY removed and/or deleted from Instagram. f) the Marketing Director of XXXXXXXXX, immediately contacted the Complainant, apologized and at the same time informed her of the above deletion/removal. 1.4.1. All the photographic and video material was acquired before 28/12/2018, when the Right of Access to Public Sector Information Law of 2017 (Law 184(I)/2017) came into force and for this reason there is no written consent form in accordance with the above law, but the consent is evident through the video material and that both you and your partners take every measure to protect the personal data of the patients. In particular, after the implementation of Law 184(I)/2017, you faithfully apply the General Regulation for the Protection of Personal Data. 1.5. After receiving your letter dated 3/7/2019 and what is mentioned in it, an Officer of the Office sent me a reply letter on 5/7/2019 requesting that the consent be sent immediately and highlighting the fact that the Complainant used your phone for downloading the video, it does not mean that he consented to further processing, i.e. sharing and/or sharing and/or posting and/or viewing the relevant video on Social Media and/or otherwise. The download of the video, by the Complainant, in which she describes details before and after the operation, cannot be considered either explicit or explicit consent. 1.5.1. Furthermore, he informed you that your reference to the Right of Access to Public Sector Information Law 2017, L.184(I)/2017, is not applicable in the present case, on the one hand because the Legislation in question has not been implemented (an extension was granted at its start until December 2020), on the other hand, even if it had been implemented, you cannot invoke it in this case, since it concerns documents held by a Public Authority and not by private individuals. 1.5.2. In addition, before the implementation of GDPR 2016/679, the Processing of Personal Data (Protection of the Individual) Law of 2001 and amendments, Law 138(I)/2001, was in force, according to which photographs are personal data and sharing/posting/publishing is a form of processing. 1.5.3. In conclusion, even if the video material was taken before the entry into force of GDPR 2016/679, the infringement which you admit took place on 22/5/2019, the date on which GDPR 2016/679 was in force. 1.6. On 9/7/2019 you sent the consent form by e-mail as well as a letter in which you state, among other things, 2 a) that you do not waive the responsibility for the obligation to Protect the Personal Data of your patients, even before the General Regulation on

the Protection of Personal Data, b) with the implementation of the new Regulation, your company shows special awareness in the protection of personal data and for this purpose new consent forms have been prepared and all necessary measures are taken for the Protection of Personal Data in accordance with provisions of the law, which the patients sign, if they wish, c) you do not deny that the video in question was published, hence the Marketing manager immediately apologized to the Complainant and immediately removed them from Instagram. d) wrongly, before the General Regulation for the Protection of Personal Data 2016 came into force, you did not keep a separate, specific form for the processing of personal data and e) in no case do you attribute any responsibility to the Complainant but consider that the said, unfortunate, event is due to a misunderstanding and you promise that this will not happen again for any of your customers. 1.6.1. In the copy of the consent you sent, the initials of the Complainant can be seen on each page and her signature on the last page. On the penultimate page of the consent, points 5 and 6 it is stated: "5. I consent to the photographing or televising of the operation(s) to be performed, including appropriate portions of my body, for medical, scientific or educational purposes, provided the pictures do not reveal my identity." "6. For purposes of advancing medical education, I consent to the addition of observations to" 1.7. On 07/17/2019 I sent you a letter stating that based on the facts in front of me and the legal analysis thereof, I judged prima facie a violation of Articles 4, 6 and 9 of GDPR 2016/679 and called you, within the framework of the right to be heard , to submit your positions and opinions regarding possible violations on your part of these provisions, as well as for what reasons you believe that any corrective measure or administrative fine should not be imposed on you based on the powers granted to me by articles 58 and 83 of GDPR 2016/679, within 2 weeks from the date of receipt of the letter. 1.7.1. In the same letter dated 7/17/2019, I asked you to inform me of the number of people you employ, either personally or through your Company, as well as your turnover and at the same time I reminded you that for a similar incident , at 1/14/2019, I sent you a warning. 1.8. In your reply letter dated 7/30/2019 and after the prima facie decision, you ask that the following be taken into account before making the final decision. 1.8.1. The publication in question was made for the purpose of promoting the turnover of your company/practice, on a specific Social Media, namely Instagram. 1.8.2. Your admission of the incident is a given as well as the fact that after the Complainant indicated that she did not give consent and that she does not wish this post to be posted, you acted immediately and it was removed. The post in question was posted for a short time. 1.8.3. Your action to post photographic and/or video material on Instagram was in no way intentional nor does it involve any fraudulent behavior. 1.8.4. This action, i.e. the sharing of the Complainant's photographic and/or video material, was done because the Complainant

initially verbally gave explicit consent to the processing of her Personal Data, with the aim of informing the public about matters of the provision of medical services. 3 1.8.5. In addition, the video recording as well as the consent form were taken before the implementation of GDPR 2016/679 and were not complete and detailed, which was corrected after the implementation of GDPR 2016/679. 1.8.6. As a company/practice you have designated a specific person who inspects any publication before it is displayed on Social Media to avoid mistakes. This fact, as you state, proves that the publication in question was made by mistake, due to a misinterpretation of the consent given by the Complainant, since it was prior to the update in accordance with the provisions of GDPR 2016/679. 1.8.7. In addition, as you mention, you apply every technical and organizational measure for the Protection of Personal Data of your patients. In summary, the following are mentioned: a) preparation of a Personal Data Protection Policy Statement, b) all your employees who process Personal Data were invited and signed a responsible statement in which they were informed about the Code of Conduct and the Personal Data Protection Policy of your company, c ) the Company Policy on cookies is posted on the website of your practice and d) all possible technical measures have been taken (access codes to computers, a separate storage area for patient files to which only a specific person has access, creation of a special patient program in which where your patient data is stored and to which only a specific person has access, etc. 1.8.8. The incident in question is an isolated fact which you have never disputed. When asked by my Office, you truthfully submitted all the true facts of the case and you didn't renounce her n your responsibility for the obligation to protect Personal Data. You are available to my Office for confirmation of what you state and express your readiness to take any corrective measure, which I deem reasonable and fair under the circumstances, in the event that the Complainant has suffered damage from the release of said material. 1.8.9. With reference to the previous incident for which I sent you a warning pursuant to Article 58 par. 2(a) of GDPR 2016/679, please state that it is diametrically opposed to the present case. You claim that in the previous case there was a separate express consent form for personal data processing for the specific purpose and in addition all necessary technical measures were taken so that the identity of the data subject cannot be directly or indirectly ascertained. 1.8.10. In addition, as you mention, XXXXXXXXXXX is a Medical Service Provider Company that operates in the territory of the Republic of Cyprus and employs 6 employees. 2. Legal Aspect: 2.1. In Article 4. par. 1 of GDPR 2016/679, it states that personal data is "any information concerning an identified or identifiable natural person ("data subject"); an identifiable natural person is one whose identity can ascertained, directly or indirectly, in particular by reference to an identifier such as a name, an identity number, location data, an online identifier or one or more factors specific to the physical,

physiological, genetic, psychological, economic, cultural or social identity of the natural person in question" while in Article 4 paragraph 2 it is stated that processing of personal data refers to "any act or series of acts carried out with or without the use of automated means, on personal data or sets of personal data, such as collecting, recording, organizing, structuring, 4 the sexual life of a natural person or storing, adapting or the alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion or destruction". In Article 4. par. 7, the person in charge of processing is referred to as "the natural or legal person, public authority, or agency or other entity that, alone or jointly with others, determine the purposes and manner of processing personal data", in Article 4. par. 11 of GDPR 2016/679 the term consent is defined "as any indication of will, free, specific, explicit and fully aware, with which the data subject manifests that he agrees, by statement or by a clear positive action, to be the subject of processing the personal data concerning it" and in Article 4. par. 15 of GDPR 2016/679 as "data concerning health" are considered the personal data which are related to the physical or mental health of a natural person , including the provision of health care services, and which disclose information about his state of health,…." 2.2. Furthermore, according to Article 9 par. 1 and 2(a) of GDPR 2016/679 "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or membership in a trade union is prohibited , as well as the processing of genetic data, biometric data for the purpose of indisputable identification of a person, data concerning health or data concerning sexual orientation" unless "the data subject has provided express consent to the processing of such personal data for one or more specific purposes……"…….. 2.3. In addition, in Article 31 of GDPR 2016/679 it is stated that "The data controller and the data processor and, as the case may be, their representatives cooperate, upon request, with the supervisory authority for the exercise of its duties" 2.4. In Reference 150 of the preamble of GDPR 2016/679 it is stated, among other things, that: "To strengthen and harmonize the administrative penalties for violations of this regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate the infringements, and the upper limit and the criteria for determining the relevant administrative fines, which should be determined by the competent supervisory authority in each individual case, after taking into account all the relevant circumstances of the particular situation, with due regard in particular to the nature, gravity and duration of the infringement and its consequences and the measures taken to ensure compliance with the obligations arising from this Regulation and to prevent or mitigate its consequences infringement.…… Where administrative fines are imposed on persons who are not undertakings, the supervisory authority should take into account the

general level of income in the Member State, as well as the financial situation of the person, when considering the appropriate amount of the fine……..” 2.5. In accordance with Article 58(2) of the Regulation, I have the authority to impose administrative sanctions that include an administrative fine pursuant to Article 83, to a data controller, in this case you, the Complainant, for violating the provisions of the Regulation. In the case of an administrative fine, the provisions of Article 83(2) of the Regulation should be duly taken into account. 3. Rationale: 3.1. In this case, it is examined whether you, the Complainant, had secured the consent of the Complainant, when the video in question was uploaded and/or shared and/or published by the official profile of the practice @XXXXXXXXX, on Instagram, on presented by the Complainant, is identified and recognized. 3.2. In the present case the Complainant has signed the relevant consent by which she accepts the use of her photographs for medical, scientific or 5

educational purposes, provided that the specific photos do not reveal

her identity, (in a free translation of the text: "I consent to the photographing or

televising of the operation(s) to be performed, including appropriate portions of my body, for

medical, scientific or educational purposes, provided the pictures do not reveal my identity".

3.3. By watching the video in question which was provided to us by the Complainant and which was not

disputed by you, one perceives that no action was taken to cover or

alteration of the Complainant's face. Her facial features

Complainant, they are clearly visible in the video, both before the operation and

and after the operation. The identity of the Complainant can immediately

ascertained and identified, by persons who know it, as the conditions of the Article

4 of GDPR 2016/679 for personal identification.

3.3.1. A consequence of the identification was the immediate recognition by people who know her

Complainant and at the same time their information that she had undergone rhinoplasty, which

concerns a special category of personal data if it concerns a health issue and

is protected by Article 9 of GDPR 2016/679.

3.4. In addition, the consent granted by the Complainant concerned the use of

of her photos for medical, scientific or educational purposes, provided that the

particular photos do not reveal her identity. The posting in question and/or

publishing and/or sharing the video on Social Media is not consistent with the purpose

of the consent granted by the Complainant, in violation of Articles 9.1. and

9.2.a) of GDPR 2016/679, since her identity is fully disclosed.

3.5. The time frame in which the video in question remained posted is relevant,

as you have over 4,000 followers on the clinic's official profile

@XXXXXXXXXX on Instagram, so even if the time period is short

remained, it may have been watched by as many as 4,000 people.

3.6. The fact that you deleted the video in question at her request

The complainant does not deny the fact that it should not have been published in the first place without them

any safeguards to identify the data subject. The video

fully discloses the identity of the Complainant since no technicality was obtained

measure to prevent or alter her face.

3.7. The fact that you have taken technical and organizational measures pursuant to GDPR 2016/679 is considered

as a positive, but at the same time it must be taken into account that these did not prevent the posting and/or

sharing and/or sharing the video in question. Instead, the violation was detected and

communicated to my Office by the Complainant herself.

3.8. The earlier case, in which I addressed you with a warning, is considered

precedent and will therefore be taken into account to the extent applicable to it. Moreover, it is

relevant since the violation concerned the unsatisfactory measures for non-recognition and

patient identification and/or disclosure.

3.9. Your company, XXXXXXXXXXXXXXXXX, of which you are the sole Director and

Secretary, employs 6 employees and despite being asked you have not provided any information

regarding your turnover.

4. Conclusion/Conclusion:

4.1. Considering the above, I have concluded that the video posted and/or

shared and/or posted and/or shared by the practice's official profile

@XXXXXXXXX on the Social Networking Media Instagram, constitutes a violation of the Articles

9.1. and 9.2.a) of GDPR 2016/679.

6

4.2. Taking into account the provisions of article 83 of the Regulation, which concerns Generals

Terms of imposition of administrative fines, when measuring the administrative fine I received

taking into account, when measuring the penalty, the following mitigating factors (a – d) and

aggravating (e – j) factors:

(a) the fact that you have also admitted as the legal controller, once

you have been informed by the Complainant that she does not wish this particular video to be found

posted on Instagram, you immediately deleted it,

(b) the fact that you have made changes to the structure of the procedures governing the operation;

of the clinic in accordance with the personal data legislation, for the purpose of

your alignment with GDPR 2016/679,

(c) the fact that the post remained published for a short period of time;

(d) the number of data subjects affected by the breach, i.e. directly

Complainant and indirectly her family,

(e) the fact that the violation concerns sensitive personal data, which is characterized

as a special category of personal data and in need of increased security measures,

(f) the fact that the violation was detected and reported by the Complainant herself,

instead of you, despite the measures you had taken to avoid such incidents

(g) the nature of the offence, which affects her personal and professional life

complainant,

(h) the extent of the infringement concerning a correspondingly large number of followers

on the official profile of the practice on Instagram, until you have deleted it

said video,

(i) the fact that you did not provide information regarding your turnover, in the context

cooperation with the supervisory authority and

(j) the fact that on 14/1/2019 a decision was made against you as, in the future, when

you post photos of patients, overlay their face or other features, with

in such a way that there is no suspicion, in any way, of its disclosure

patient identity.

Based on the above, I have decided to impose on you a fine of fourteen

Thousands of Euros (€14,000)

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character