[doc. web no. 9843603]

Injunction against the company Poliambulatorio Radiologico "il Sorriso" S.r.l. - November 10, 2022

Register of measures

no. 372 of 10 November 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, prof.ssa Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, components and the cons. Fabio Mattei, general secretary;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as well as on the free circulation of such data and repealing Directive 95/46 /CE, "General Data Protection Regulation" (hereinafter "Regulation");

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196 "Code regarding the protection of personal data", containing provisions for the adaptation of national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons with regard to the processing of personal data, as well as to the free movement of such data and which repeals Directive 95/46/EC (hereinafter the "Code");

CONSIDERING the Regulation n. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved with resolution no. 98 of 4/4/2019, published in the Official Gazette no. 106 of 8/5/2019 and in www.gpdp.it, doc. web no. 9107633 (hereinafter "Regulation of the Guarantor n. 1/2019");

Given the documentation in the deeds;

Given the observations made by the general secretary pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web no. 1098801;

Speaker Prof. Pasquale Stanzione;

WHEREAS

1. The complaint

On the 20th date, the Authority received a complaint formulated against the company Poliambulatorio Radiologico "il Sorriso"

S.r.l., located in Noviglio/Binasco (MI) in Via Dante Alighieri 1 - VAT number 10481700960 (hereinafter "Company"), with which the complainant complained that, once she went "to the medical center for a visit to the entrance (...) (she) was asked to "sign for privacy" on a tablet, with only the space for the signature, without that any text could be displayed" and that upon repeated requests to know the text of the information regarding the processing of personal data, it was provided "as information (an) e-mail (...) printed at the time (...)" called “Consent to the processing of personal data pursuant to art. 7 of the GDPR 2016/679".

The complainant also pointed out that "the contact details of the DPO are not recognized and also on the site the privacy policy does not even mention health data".

2. The preliminary investigation

In relation to what is represented in the complaint, the Office, with notes of the XX (prot. n. XX) and of the XX (prot. n. XX), requested, pursuant to art. 157 of the Code, to provide some elements useful for the evaluation of the relevant profiles in the field of personal data protection and, in relation to this request, the Company itself, through its lawyer, has declared, among other things, that:

- "the Structure (...), at its entrance and in good evidence for each check-in station, has displayed the model for consent to the processing of personal data pursuant to art. 7 GDPR 679/2016 (…). This circumstance is confirmed by the attached photographic documentation from which it can easily be seen how, just below the tablets for signing the model itself, two printouts of the consent to the treatment are positioned, permanently and periodically updated, one for each acceptance station (...)";
- "With reference to the information that the registered Company provides to the interested parties, pursuant to art. 13 of the Regulation, it should be noted that adequate information is given on the content of the model of consent to the processing of personal data by posting it, at each user acceptance point, by displaying the form itself";
- "Said form, to which the user consents to the processing by signing graphics collected on the tablet, is simultaneously sent by e-mail to the adhering subject. At the same time, the staff in charge illustrate the circumstance to the user, warning that the graphic signature on the tablet is necessary to give consent to the processing of personal data. Therefore, the methods through which adequate information is provided to users are both graphic (...) and verbal";
- “Further false is the circumstance declared by the complainant that ... also on the site the privacy policy does not even

mention health data. This circumstance is easily denied by the mere production of the privacy policy extracted from the link https://www.iubenda.com/privacy-policy/53698927 of the website https://www.centroradiologicoilsorriso.it/ (doc. 5) which shows easily the exact and exhaustive information required by the European Privacy Regulation EU/2 016/679 (GDPR)";

- "The graphometric signature of the document is collected via tablet in compliance with the provisions of the Digital Administration Code (...) and the security in the storage of documents is guaranteed by an encryption system based on the AES-256 algorithm and the information itself is sent a copy via email to the customer (confirmed by the complainant)";

- "In no case are biometric data also acquired which, where processed, are so in accordance with art. 9 of the Regulation, paragraph 3 and 2 letter h) by or under the responsibility of a professional subject to professional secrecy in accordance with Union or Member State law or with the rules established by the competent national bodies or by another person also subject to the obligation of secrecy in accordance with the law of the Union or of the Member States or with the rules established by the competent national bodies";

- "the Il Sorriso S.r.l. Radiological Clinic, as a private facility and as, clarified by the same registered Body with the clarifications released on the XX Register of measures n. XX of the XX, is not subject to the obligation of the appointment of the DPO as the data processing that takes place does not take place on a large scale. Nonetheless and due to the type of data processed, the Il Sorriso S.r.l. Radiological Clinic, since its establishment in June XX, has deemed it necessary to equip its structure with the figure of the Data Processing Manager as identified above (...) It should be noted that the The Data Protection Officer is il Sorriso S.r.l. (…) in the person of the Sole Director and l.r.p.t. Gardinazzi Alessandro (…)". Attached to the acknowledgment note, the Company has produced, in addition to some photographs regarding the positioning of the model called "Consent to the processing of personal data pursuant to art. 7 of the GDPR 2016/679" at the polyclinic counters, a copy of the latter document and a copy of the one concerning the "privacy policy of www.centroradiologicoilsorriso.it." .

With reference to what emerged, taking into account that, from the examination of the documentation examined, the described conduct was not compliant with the relevant regulations on the protection of personal data, the Office, with deed dated XX (prot. n. XX) , notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation, inviting the latter to produce defense writings or documents to the Guarantor or to ask to be heard by the Authority (art. 166, paragraphs 6 and 7, of the Code, as well as art. 18, paragraph 1, law n. 689 of the November 24, 1981)

In particular, the Office, in the aforementioned deed, considered that the Company:

- has not provided the interested parties, within the context of the aforementioned model made available to them, some of the elements required by art. 13 of the Regulation, in violation of the articles 5, letter. a) (principle of "lawfulness, correctness and transparency" of the processing of personal data) and 13 of the Regulation ("Information to be provided if personal data are collected from the interested party");

- has processed biometric data collected through the affixing, by the interested parties, of the graphometric signature on the tablet in the absence of a legitimizing prerequisite; this, in violation of the articles 5, letter. a) and c) (principles of "lawfulness, correctness and transparency" and "data minimization") and 9 of the Regulation ("Processing of particular categories of personal data");

- has not proceeded to designate the Data Protection Officer in compliance with the provisions of the Regulation, nor to the subsequent publication on its website, of the contact details of the same and to the relative communication to the Guarantor; this, in violation of the art. 37 of the Regulation.

Following the aforementioned act of notification of violation, the Company, with note dated XX, sent the defense briefs, pursuant to art. 166, paragraph 6, of the Code, declaring, among other things, that:

- "with reference to the disputed violation of art. 13 of the Regulation due to the alleged absence of certain information to be provided to interested parties (...), in compliance with art. 13 of the Regulation, the information referred to in the relative provision is correctly provided, it being clearly indicated that the processing is carried out for a period of time "...not exceeding that necessary for the purposes for which they were collected" thus determining, the criterion used to determine the period as clarified by the same Guarantor in the event there is no regulatory provision that provides for retention terms, in which case the data controller is required to identify the retention period of data relating to health from which the identity of the interested party can be obtained for the time necessary (and no longer) to achieve the purposes of the processing";

- "in compliance with the regulatory provisions, the correct indication of the subject against whom to exercise the "rights of the interested parties" pursuant to articles from 15 to 22 of the Regulation and the relative modalities as it is not necessary to indicate the contact details of the Data Protection Officer (art. 13, letter b) given that, (…), the applicant falls into those categories for which, the same Guarantor, has clarified that they are not obliged to appoint the DPO, as the data processing they carry out does not take place on a large scale";

- "with reference to the affixing of the "graphometric signature" on the tablet, it is believed that the applicant has not committed a violation since, due to the type of equipment used and collection methods, the relative information is not required from the interested parties not since there is some evidence of their biometric data (…). With reference to the disputed violation of art. 9 of the Regulation "Processing of biometric data in the absence of a legal basis" (...), the applicant uses "MediStudio" management software, created by the company Medinformatica S.r.l. (…) in compliance with EU Regulation 2016/679, regarding the protection of personal data ("GDPR"). This software uses the simple signature collected with the WACOM STU-430 tablet which is decompiled into base64 and saved directly into the password protected database. Therefore, the applicant does not have folders with signatures saved in readable format as there is no retention of the affixed signature or usability of the same or of the resulting biometric data";

- "It is quite clear that, since these are applications that operate locally, in "client/server" mode, these do not allow the Company to access in any way the data (personal or otherwise) stored in them by the Customer".

Subsequently, on the 20th date, the hearing requested by the Company was held, during which it was declared that:

- "in addition to what is already in the documents, it is specified that in total good faith the party had not deemed the appointment of the DPO necessary; despite this, in the month of XX it proceeded to entrust this task to Ms Cattaneo, waiting to designate an external subject starting from the month of next September. This external subject will carry out a complete audit on all the profiles relating to the protection of personal data";

- "in consideration of the recent appointment of Ms Cattaneo as DPO, the communication of her contact details to the Authority has not yet taken place, with the reservation, however, of providing for this fulfillment as soon as possible" ;

- "in relation to the use of the handwritten signature on the tablet, as already specified in the defense brief sent, it should be noted that there is no collection of biometric data";

- "lastly, it is important to point out that the outpatient clinic has recently opened (XX) and to date has received around 55,000 users without any objection ever being raised" (see report no. XX of the XX).

On the basis of what has been declared, the Company has requested the dismissal of this proceeding and, alternatively, the application of a fine as small as possible.

3. Outcome of the preliminary investigation

On the basis of the statements made to the Authority during the proceedings, as well as the examination of the documentation

acquired, the following has been ascertained.

3.1 The correctness and transparency of the treatment: information to be provided to the interested parties

In compliance with the principle of "lawfulness, correctness and transparency", the data controllers, must adopt appropriate measures to provide the interested party, before starting the treatment, with all the information required by the Regulation in a concise, transparent, intelligible and easily accessible form , with simple and clear language (articles 5, paragraph 1, letter a), 12 and 13 of the Regulation; with specific reference to the information to be provided to the interested party, as part of the activity carried out by data controllers operating in the health sector, see also, the par. 2 of the Provision of 7 March 2019, n. 55, doc. web no. 9091942, containing "Clarifications on the application of the regulations for the treatment of data relating to health in the health sector"). The aforementioned obligation does not exist only if, and to the extent that, the interested party already has the information (Article 13, paragraph 4).

An examination of the documentation in the records shows that the information on the processing of personal data provided to data subjects does not include all the elements required by the Regulation to ensure correct and transparent processing.

In particular, the Authority has ascertained that the Company has failed to provide a series of elements required by the same Regulation, essential for achieving the objective of transparency underlying the fulfillment, such as those relating to the right to lodge a complaint with the Supervisory Authority , the indication of the retention period of the information or the criteria used to determine this period as well as the contact details of the Data Protection Officer (Article 13, paragraph 1, letter b) and 2, letter a), and d) of the Regulation).

In this regard, in fact, with reference to the indication of the data retention period, the deduction by the Company in the defense brief cannot be shared, regarding the circumstance that the wording "the processing is carried out for a period of time" ... not exceeding that necessary for the purposes for which they were collected"" can integrate the provision contained in the art. 13, par. 2, lit. a) of the Regulation (according to which information on the data retention period can be provided by the data controller also by indicating the criteria used to determine it (art. 13, paragraph 2, letter a), of the Regulation).

In fact, this wording does not add any information with respect to the explanation of the principle of limitation of data retention, set out in art. 5, par. 1, lit. e) of the Regulation, according to which the data must be "kept in a form that allows the identification of the interested parties for a period of time not exceeding the achievement of the purposes for which they are processed".

In the same sense, according to what is indicated in the Annex to the Guidelines on transparency pursuant to Regulation

2016/679 - drawn up by the Art. 29 Group and adopted on November 29, 2017 as well as, in the amended version, on April 11, 2018 (WP260 rev .01) - containing "Information to be provided to the interested party pursuant to article 13 or 14", the retention period (or the criteria for determining it) "should be indicated in such a way as to allow the interested party to establish what it will be, in based on your specific situation, the period foreseen for the specific data/purposes. It is not sufficient for the data controller to state in a general way that personal data will be kept for as long as it is necessary for the legitimate purposes of the processing. Where relevant, different retention periods should be set for different categories of personal data and/or purposes of processing, including, where appropriate, archiving periods.

As for the information relating to the exercise of the rights referred to in Articles from 15 to 22 of the Regulation, although the minimum disclosure obligation required by art. 13, par. 2, lit. b), of the same Regulation, it is deemed appropriate that its content be specified, in a more exhaustive way, in order to facilitate this exercise; this, in line with the art. 12, par. 2, of the Regulation according to which "the data controller facilitates the exercise of the rights of the interested party" and in compliance with Recital n. 39 of the same Regulation, regarding the appropriate clarification of the methods through which to exercise these rights. In fact, also according to what is reported on the point in the Annex to the Guidelines on transparency mentioned above, "the information should be specific to the hypothesis of treatment and include a summary of the nature of the rights, of the way in which the interested party can take steps to exercise them and their possible limitations (..). In particular, the right to object to the processing must be explicitly brought to the attention of the interested party at the latest at the time of the first communication and must be presented in a clear and separate form from any other information. Similarly, it is recognized the opportunity to rename, in accordance with art. 13 of the Regulation, the document containing "Consent to the processing of personal data pursuant to art. 7 of the GDPR 2016/679", also re-evaluating the cases in which the "consent" was indicated as a legal basis for the processing (in relation to this, in fact, for example, pursuant to the Regulation, the consent of the interested parties does not it is required for the processing of health data necessary for health care purposes (Article 9, paragraph 2 letter h) and paragraph 3 of the Regulation and in this sense, also the provision of the Guarantor of 9 March 2019, doc web 9091942, containing "Clarifications on the application of the regulations for the treatment of data relating to health in the health sector").

As illustrated above, the treatment of patients' personal data put in place by the Company cannot be considered compliant with the principle of lawfulness, transparency and correctness, nor with the obligation in terms of information to the interested

parties, since the information provided to them is incomplete (art. 5, paragraph 1, letter a) and 13 of the Regulation).

3.2 The obligations regarding the designation of the Data Protection Officer

The designation of the Data Protection Officer constitutes a measure aimed at facilitating compliance with the data protection regulations, which is mandatory when the specific conditions referred to in art. 37 of the Regulation.

This provision provides that "The data controller and the data processor systematically designate a data protection officer whenever: (...) the main activities of the data controller or the data processor consist in the processing, on a large scale, of particular categories of personal data referred to in Article 9 (…)" (Article 37, paragraph 1, letter c) of the Regulation).

In explication of this rule, the Guidelines on Data Protection Officers - WP 243/2016, recommend taking into account some factors in order to establish whether the main activities of the data controller consist of a treatment carried out on a large scale, such as the number of interested parties, the volume of data and/or the different types of data being processed, the persistence of the processing activity, the geographical scope of this activity (see point 2.1.3. of the aforementioned Guidelines, updated on 5 April 2017, which can be found at https://ec.europa.eu/newsroom/article29/items/612048).

The aforementioned conditions, as also indicated by the Authority through FAQs published on its website (https://www.garanteprivacy.it/faq in the "RPD" sections and, therein, "RPD in the private sphere", adopted in addition to those attached to the Guidelines WP 243/2016), are also used for companies operating in the sector of health care, health prevention/diagnostics such as private hospitals, spas, medical analysis laboratories and rehabilitation centres.

In the case in question, from the information relating to the Company, which can be found on the latter's website (https://www.centroradiologicoilsorriso.it/storia/), it appears that the Company itself offers a territorial service oriented towards prevention and diagnosis in private scheme consisting of a wide range of services and benefits for prevention, diagnosis and therapy in numerous fields of medicine (allergology, andrology, angiology, cardiology, dermatology, diabetology, endocrinology, physiatry, gastroenterology, geriatrics, gynecology and obstetrics, naturopathy, neurosurgery, neurology, nutrition, ophthalmology, osteopathy, orthopaedics, orthoptics, ENT, paediatrics, pulmonology, rheumatology, breasts, urology). In particular, in addition to the aforementioned specialist visits, it offers "diagnostic imaging, psychological centre, sports medicine, physical medicine and rehabilitation" services as well as a "withdrawal point"; this, through a group of about 70 professionals including medical specialists, health technicians, nurses, office workers. Therefore, in the light of the foregoing, the main activity of the Company itself, also due to the high volume of data relating to health processed in the

context of the numerous and diversified medical activities carried out, involves the treatment, on a large scale, of details of personal data pursuant to art. 9 of the Regulation (see also point 3 of the Authority's Provision no. 55 of 7 March 2019, web doc. no. 9091942, relating to the clarifications provided by the Guarantor on the application of the regulations for the processing of data relating to health in health sector) and, for these reasons, the Company is to be held required to comply with the obligations established by the Regulation in relation to the figure of the Data Protection Officer.

That said, having acknowledged the Company's declarations regarding the designation of the aforementioned Data Protection Officer, it should be noted that, in relation to the Company's declaration that "the Data Protection Officer is the Il Sorriso Radiology Clinic S.r.l. (…) in the person of the Sole Director and l.r.p.t. (...)", the Regulation establishes that this Manager "(...) may be an employee of the data controller or of the data processor or perform his duties on the basis of a service contract" (art. 37, paragraph 6, of the Regulation). The controller and the processor ensure that the Data Protection Officer "(…) does not receive any instructions regarding the performance of these tasks" and, if he performs other tasks and functions within the organizational structure in which is called to operate as Data Protection Officer, they also ensure that "these tasks and functions do not give rise to a conflict of interest". In fact, the "data protection officers, employees or otherwise of the data controller, should be able to fulfill the functions and tasks assigned to them independently" (Recital 97 of the Regulation). "The data protection officer reports directly to the hierarchical top of the data controller and the data processor" (Article 38 of the Regulation. See, in this sense, also https://www.garanteprivacy.it/faq in the sections "DPO" and, therein, "DPO in the private sector", adopted in addition to those attached to the Guidelines WP 243/2016 updated on 5 April 2017, at https://ec.europa.eu/newsroom/article29/items /612048). This highlights that the Regulation requires that the Data Protection Officer occupy an independent and distinct position within the organizational structure in which he operates, above all with respect to especially directive functions, as also foreseen by point 3.5 of the WP Guidelines 243/ 2016 updated on 5 April 2017, in https://ec.europa.eu/newsroom/article29/items/612048/en, "" ("a DPO cannot play, within the organization of the data controller or the data controller, a role that involves defining the purposes or methods of processing personal data (…) There may be situations of conflict of interest within the organization of the data controller or data processor with regard to managerial roles (managing director, operations manager, financial manager, healthcare manager, marketing manager, human resources manager, IT manager), but also with respect to hierarchically lower positions if the latter involve determining the purposes or means of the processing).

In light of the above, it appears that the Company has designated a Data Protection Officer not in compliance with the provisions of the Regulation and, in any case, has not published the contact details of the same on its website, nor has it communicated them to this Authority, in violation of art. 37, as also resulting from a check carried out by the Office on the Company's website "https://www.centroradiologicoilsorriso.it/", as well as in the DPO register of the Office itself. This non-compliance, contrary to the commitment declared by the data controller during the hearing, is persistent at the time of the adoption of this provision.

3.3. Processing of biometric data

In relation to the hypothesized processing of personal data of a biometric type, acquired through the signing of documentation by means of a graphometric signature, we acknowledge the declarations of the Company, also confirmed during the hearing of the XX, according to which with the signing of electronic documents biometric data are collected based on the detection of the dynamics of affixing the handwritten signature (graphometric signature) of the interested parties: reference is made, in particular, to the dynamic parameters associated with the act of signing, such as, for example, tracking speed, acceleration , the pressure, the inclination, the jumps in flight.

4. Conclusions

In light of the above, taking into account the statements made by the data controller during the preliminary investigation, as well as what emerged from the documentation acquired and considering that, unless the fact constitutes a more serious crime, anyone, in a proceeding before the Guarantor , declares or falsely certifies news or circumstances or produces false deeds or documents, he/she is liable pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the duties or the exercise of the powers of the Guarantor", the elements provided by the data controller do not allow to fully overcome the findings notified by the Office with the act of initiation of the proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

Therefore, the relevant preliminary assessments of the Office are confirmed and the illegality of the processing of personal data carried out by the Company is ascertained, in violation of articles 5, par. 1, lit. a), 13 and 37 of the Regulation, in the terms referred to in the justification.

5. Corrective measures (Article 58, paragraph 2, letters d) and f), of the Regulation).

The art. 58, par. 2, lit. d), of the Regulation provides that the Guarantor has the corrective powers to "order the data controller

or the data processor to bring the processing into line with the provisions of this Regulation, where applicable, in a specific manner and within a specific term".

In this context, in the light of the rules indicated, it is deemed necessary, due to the failure to implement the obligations required by the Regulation, pursuant to art. 58, par. 2, lit. d), of the Regulations, to establish that the "il Sorriso" S.r.l. Radiology Clinic provides:

- the integration of the information provided pursuant to art. 13 of the Regulation with the missing elements relating to the indication: of the contact details of the Data Protection Officer, of the retention times or of the criteria used to determine this period, of the right to lodge a complaint with the Supervisory Authority (art. 13 , paragraph 1, letter b) and par. 2, lit. a) and d) of the Regulation);

- to the designation of the Data Protection Manager with the third party characteristics indicated above, in compliance with the provisions of articles 37 et seq. of the Regulation, by communicating to this Authority its contact data (following the specific procedure available on the Guarantor's website at the address https://servizi.gpdp.it/comunicazionerpd/s/), as well as arranging for the publication of such data on the institutional website, pursuant to art. 37, par. 7 of the Regulation, considering that at the time of the adoption of this provision, this obligation has not yet been fulfilled.

6. Adoption of the injunction order for the application of the pecuniary administrative sanction and accessory sanctions (articles 58, paragraph 2, letter i and 83 of the Regulation; article 166, paragraph 7, of the Code).

The violation of the articles 5, 13 and 37 of the Regulation, determined by the processing of personal data carried out by the Company, which is the subject of this provision, is subject to the application of the administrative fine pursuant to art. 83, par. 4, lit. a) and par. 5, letter. a) of the Regulation.

It should be considered that the Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, has the power to "impose a pecuniary administrative sanction pursuant to article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, according to the circumstances of each single case" and, in this context, "the College [of the Guarantor] adopts the injunction order, with which it also orders the application of the ancillary administrative sanction of its publication, in whole or in part, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code" (art. 16, paragraph 1, of the Guarantor's Regulation no. 1/2019).

The aforementioned pecuniary administrative sanction imposed, depending on the circumstances of each individual case,

must be determined in the amount taking into account the principles of effectiveness, proportionality and dissuasiveness, indicated in art. 83, par. 1, of the Regulation, in the light of the elements provided for in art. 83, par. 2 of the Regulation in relation to which, in particular, it is noted that:

- the data processing carried out by the Company concerns information relating to the health of a potentially large number of patients (Article 83, paragraph 2, letters a) and g) of the Regulation);
- the violation relating to the obligations established by the Regulation on the designation of the Data Protection Officer and aimed at making all the information pursuant to art. 13 of the Regulation, date back at least to the opening date of the structure which, according to what was declared by the data controller during the hearing, took place in the month of June of the year XX (art. 83, paragraph 2, letter a) of the Regulation);
- the Company did not demonstrate full cooperation with the Authority both during the preliminary investigation - for not having provided an exhaustive reply to the initial request for information formulated by the Authority - and following the initiation of the procedure pursuant to art. 166 of the Code, not having remedied the notified violations (art. 83, paragraph 2, letters c) and f) of the Regulation);
- there are no previous violations committed by the data controller (Article 83, paragraph 2, letter e) of the Regulation);
- the Company, which started its activity in June 2020, has not received, to date, any objection, except for the one that is the subject of the present proceeding (art. 83, paragraph 2, letter k) of the Regulation).

Based on the aforementioned elements, considered as a whole and taking into account the economic conditions of the Company, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 4 and 5, lett. a) of the Regulation, to the extent of 15,000 (fifteen thousand) euros for the violation of articles 5, 13 and 37 of the Regulation as a pecuniary administrative sanction, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed, in consideration of the volume and nature of the data processed, that the ancillary sanction of publication on the website of the Guarantor of this provision should be applied, provided for by art. 166, paragraph 7, of the Code and art. 16 of the Regulation of the Guarantor n. 1/2019.

Finally, it should be noted that the conditions pursuant to art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

ALL THIS CONSIDERING THE GUARANTOR

notes the illegality of the processing of personal data carried out by the company Poliambulatorio Radiologico "il Sorriso" S.r.l. for the violation of the articles 5, 13 and 37 of the Regulation in the terms referred to in the justification;

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the company Poliambulatorio Radiologico "il Sorriso" S.r.l., located in Noviglio/Binasco (MI) in Via Dante Alighieri 1 – VAT number 10481700960 to pay the sum of 15,000.00 (fifteen thousand) euros, by way of administrative fine pecuniary for the violations indicated in the justification; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within the term of thirty days, an amount equal to half of the fine imposed;

ENJOYS

to the "il Sorriso" S.r.l. Radiological Outpatient Clinic:

a) to pay the sum of 15,000.00 (fifteen thousand) euros, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, according to the methods indicated in the attachment, within thirty days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the law no. 689/1981;

b) pursuant to art. 58, par. 2, lit. d), of the Regulation, to integrate the information provided pursuant to art. 13 of the Regulation with the missing elements relating to the indication: of the right to lodge a complaint with the Supervisory Authority, of the retention period of the information or of the criteria used to determine this period, as well as the contact details of the Data Protection Officer (Article 13, paragraph 1, letter b) and 2, letter a) and d) of the Regulation);

c) pursuant to art. 58, par. 2, lit. d) of the Regulation, to designate the Data Protection Officer with the third party character indicated in the justification, in compliance with the provisions of articles 37 et seq. of the Regulation, notifying this Authority of the contact data of the same (following in this regard the specific procedure available on the website of the Guarantor at the address https://servizi.gpdp.it/comunicazionerpd/s/), as well as arranging the publication of such data on its website, pursuant to art. 37, par. 7, of the Regulation;

d) pursuant to articles 58, par. 1, lit. a), of the Regulation and 157 of the Code, to communicate to this Authority, providing an adequately documented response, within thirty days of notification of this provision, the initiatives undertaken in order to implement the above orders pursuant to the aforementioned art. 58, par. 2, lit. d) of the Regulation.

HAS

- pursuant to art. 166, paragraph 7, of the Code and by art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019, the publication of this provision on the Guarantor's website, considering that the conditions set forth in art. 17 of the Regulation of the Guarantor n. 1/2019;

- annotation of this provision in the internal register of the Authority, provided for by art. 57, par. 1, lit. u), of the Regulation, of the violations and of the measures adopted in accordance with art. 58, par. 2, of the Regulation.

Pursuant to art. 78 of the Regulation, of the articles 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision it is possible to lodge an appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the appellant resides abroad.

Rome, 10 November 2022

PRESIDENT

station

THE SPEAKER

station

THE SECRETARY GENERAL

Matthew