[doc. web n. 9734884]

Injunction order against the Gaetano and Piera Borghi Foundation Nursing Home - December 2, 2021

Record of measures

n. 422 of 2 December 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

GIVEN the Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46 / EC, "General Data Protection Regulation" (hereinafter the "Regulation");

GIVEN the legislative decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national system to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of individuals with regard to to the processing of personal data, as well as to the free circulation of such data and which repeals Directive 95/46 / EC (hereinafter the "Code");

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

GIVEN the documentation in the deeds;

GIVEN the observations made by the Secretary General pursuant to art. 15 of the Guarantor Regulation n. 1/2000 on the organization and operation of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web n. 1098801;

Rapporteur Prof. Ginevra Cerrina Feroni;

WHEREAS

1. The violation of personal data.

With a note from the twentieth century, the Gaetano e Piera Borghi s.r.l. (hereinafter "Nursing home") notified the Guarantor,

pursuant to art. 33 of the Regulation, a violation of personal data in relation to a computer attack attributable to the hacker group LulzSec_ITA, which resulted in the publication, on the Twitter profile of the same group, of radiological images attributable to the nursing home, declaring to have become aware of the described episode on XX, following communication from the postal police.

In particular, the nursing home represented that "a person who qualified as a hacker and called LulzSecITA, published the following message on his Twitter account:" A lot of money spent in healthcare, and then our private and sensitive data, are protected by passwords by default. How disgusting". From checks immediately requested from the Data Processing Manager - System Administrator Med Store Saranno S.r.l., appointed by the XXth Act (...), it emerged that from the screen that should have allowed only the doctors belonging to the Foundation to access remote to diagnostic tests, this measure introduced on the XXth as part of the anti-gathering measures to deal with Covid, it was possible to access the data using default and non-dedicated passwords, thus making access to data not impossible. In particular, from the aforementioned checks on the log files carried out by the aforementioned manager, it emerged that only one frame of radiological investigation of an interested party was viewed by the hacker (the complete investigation is composed of a plurality of images) and the radiography of other interested, without being able to see in both cases any report, as it is not accessible from the web. In any case, the publication on Twitter took place by obscuring the surname and any other data useful for identification. The aforementioned responsible admitted the incident, assuming responsibility for the same and stating that he had immediately removed the causes. (…). The Foundation's lawyer will take the necessary steps towards the Data Processor ".

In the aforementioned notification it was also highlighted that the violation would have involved users of laboratory diagnostics and that the nursing home, at the time, did not believe that the conditions for the communication pursuant to art. 34 of the Regulation. It has, in fact, considered the probable consequences “null for the interested parties, as the access allowed to identify only the name and surname, but not other data such as to identify the subject in a univocal way; not even the name of the Borghi Foundation was discovered. In essence, the data revealed only concerned that a person with a certain name and surname carried out a diagnostic test in a health facility, without it being possible to uniquely identify either one or the other ".

2. The preliminary activity.

Following the aforementioned notification, the Office asked the Nursing Home to provide some useful elements for the evaluation of profiles in the field of personal data protection (note of XX prot. No. XX).

The Nursing Home provided feedback, also on the basis of the clarifications provided by the data controller, stating that "this group [hackers, n.d.a.] managed to enter the public IP [...] specifically it was not used for the configuration the standard port "80" but the NON STANDARD port "88", only at this point did he find access to "admin" "admin" […] The radiologist has always used this password for access ". As regards, then, the measures adopted to remedy the violation of personal data and to mitigate the possible negative effects on the interested parties, the Nursing Home stated that "the Data Processor confirms in his communications that he has replaced access passwords immediately after receiving the notification "and that" the adoption of the secure HTTPS protocol has been commissioned and will be implemented in the technical times strictly necessary "(see note of XX points c), d) and h)) .

In relation to what was communicated by the Nursing Home, the Office, with deed of XX prot. n. XX, initiated, pursuant to art. 166, paragraph 5, of the Code, with reference to the specific situations of illegality referred to therein, a procedure for the adoption of the measures referred to in art. 58, par. 2 of the Regulation, towards the nursing home, inviting it to produce defensive writings or documents to the Guarantor or to ask to be heard by the Authority (Article 166, paragraphs 6 and 7, of the Code, as well as Article 18, paragraph 1, l. no. 689 of 24 November 1981).

In particular, the Office, in the aforementioned deed, preliminarily represented that:

- the information subject to the violation constitutes personal data relating to health, which deserve greater protection since the context of their processing could create significant risks for fundamental rights and freedoms (Cons. no. 51);
- the rules on the protection of personal data establish that the same data must be "processed in a manner that guarantees adequate security (...), including protection, by means of adequate technical and organizational measures, from unauthorized or illegal processing and from accidental loss, destruction or damage ("integrity and confidentiality") "(Article 5, paragraph 1, letter f) of the Regulations);
- with regard to the security of personal data, the data controller and the data processor must implement adequate technical and organizational measures to ensure a level of security appropriate to the risk, "taking into account the state of the art and the costs of implementation , as well as the nature, object, context and purpose of the processing, as well as the risk of varying probability and gravity for the rights and freedoms of individuals "(...). "In assessing the adequate level of security, particular account is taken of the risks presented by the processing that derive in particular from the destruction, loss, modification, unauthorized disclosure or access, accidentally or illegally, to data personal data transmitted, stored or otherwise processed

"(Article 32 of the Regulation);

- from the examination of the documents in place, some critical issues emerged relating to the obligations regarding the security of the processing, with particular reference to the use of unsecured network protocols and the failure to define a password policy;

• in relation to the first profile, at the time of the violation, the installation aimed at allowing the radiologist to view the images to be reported, carried out remotely on the 20th, allowed access to the MED Dream software - DICOM viewer designed for diagnosis, display, storage and transmission of medical images usable through a web browser and an access password - on http protocol (hypertext transfer protocol), a network protocol that does not guarantee the integrity and confidentiality of the data exchanged between the user's browser and the server that hosts the service / website and does not allow users to verify the authenticity of the server to which they connect;

• as for the second profile, at the time of the violation, access to the MED Dream software by the radiologist was carried out with an administrative user (admin) and a non-robust password (admin).

In the aforementioned deed, it was therefore highlighted that the failure to use cryptographic tools for data transmission and access to the MED Dream software in the absence of checks on the quality of the passwords used - for technical users and for users in use at authorized subjects -, of measures for the mandatory modification of the same on first use or, in any case, periodically, as well as of automatic user blocking mechanisms, did not comply with the provisions of art. 5, par. 1, lett. f) and art. 32 of the Regulation, taking into account the nature of the data in question (also relating to health) and the high risks deriving from their possible acquisition by third parties.

Having said that, on the basis of the elements in the file, with the aforementioned note of the XXth, the Office considered that, at the time the personal data violation occurred, the Nursing Home had carried out a treatment in violation of the obligations in security of treatment referred to in art. 32 of the Regulation and the basic principles referred to in Article 5 of the same Regulation.

With a note of the twentieth, the nursing home sent its defense briefs, accompanied by specific documentation, in which, in particular, after having described the matter in question, it was represented that:

a) "The image processing was done using the MED Dream software, designed, supplied and installed by the company Med Store Saronno S.r.l., appointed as Data Processor with a written document dated the XXth (...). On the home page of the

aforementioned Manager, the software provided is described as follows:

“MedDream is a DICOM viewer designed for diagnosis, visualization, archiving and transmission of medical images; medDream has been designed for a real support to the professional doctor in the daily decision-making process, connecting all medical data in a single and fast network; medDream provides a fast and reliable way to search, view and analyze medical images, signals and video files on various devices: computers, smartphones, tablets and so on. The medDream DICOM Viewer is FDA approved for diagnostic use, CE certified as a medical device, and can be used for primary diagnosis or even review purposes. The viewer has been designed for fast distribution and without the need for installation, a web browser and an access password are enough ";

b) "the necessary checks and verifications were immediately requested from the Data Processing Manager, whose legal representative (..) replied on XX" declaring: to be "very sorry (o) for unauthorized access by part of hackers who have, I don't know how, identified your property's IP. The installation in your center was carried out remotely on the 20th in full COVID emergency to allow the radiologist to view the DICOM images remotely. In the unauthorized accesses that we encountered, some images were displayed which were then tweeted "; "Since there is no sensitive patient data in the system (medDream is only a viewer of radiological images), the Hacker on duty immediately lost interest in our system and immediately turned elsewhere"; “We have analyzed the LOGs since they were installed and in particular on May 24th and 26th and they are not accessed except those of authorized radiologists. On the 25th at 11.50am we recorded very fast and uncommon accesses to radiologists who normally report the entire study consisting of hundreds of images. In these short logins, the individual images (not the whole study) of the patients indicated on Twitter were displayed. In the afternoon, as confirmed by the radiologist, we replaced all the passwords and blocked all access possibilities ”; "The technology used in medDream does NOT allow data to be saved locally, all data is deleted when you log out"; "In our medDream viewer there are NO other sensitive data besides Name Surname Sex and date of birth of the patient but not visible in the message posted on the network"; “In our installations the procedure provides, in addition to the access passwords customized for each radiologist, protection in HTTPS (SSL certificate). To do this it is necessary to associate your public ip address (… ..) to a web domain and consequently purchase an SSL certificate for the domain itself. Once we have obtained the private key and the certificate, we are able to configure the web server where the MedDream application resides, to respond to the HTTPS protocol ”; "Now the emergency is over, if you agree with our proposal, we can proceed with the above".

c) "Med Store has fully recognized its responsibilities in the event", also following requests for clarification relating to the procedure for assigning credentials;

d) "the legal representative of Med Store S.r.l. clarified the following regarding the credentials attribution procedure: "This group [the hackers, n.d.a.] managed to enter the public IP of your client, identified with a specific hacking activity, specifically it was not used for the configuration the standard port "80" but the NON STANDARD port "88", only by arriving at this point did it find the access "admin" "admin". Certainly an activity that cannot be performed by normal web users; (...) the medDream software displays the images, no reports, interpretations or anything else sensitive to the patient. The radiologist has always used this password for access "";

e) "the Data Processor confirms (...) that he has replaced the access passwords immediately after receiving the report";

f) "On the point of the authorization profiles, the Data Processor specified as follows:" The procedure provides for the assignment to the radiologist of a USER ID and PASSWORD. The USER ID is associated with the name of the radiologist while the PASSWORD (is) composed of upper and lower case characters and at least one number. Access is also available through USERID and Password generated by your customer's domain in LDAP, using the security policies of your client "";

g) "following the events, the Foundation has commissioned the adoption of the secure HTTPS protocol, which will be implemented at the same time as any additional requirements that may emerge following the outcome of this procedure";

h) with reference to art. 83, par. 2, lett. a) of the Regulations “it is believed that the violation - if deemed to exist - is certainly particularly tenuous. In fact, it also emerges from the log files that: a) only one frame of radiological investigation of an interested party was viewed by the hacker, while the complete investigation - the only one that allows some evaluation to highly qualified personnel - is composed of a plurality of images; b) the radiograph of only one other person concerned was viewed; c) in both cases no one was able to see any report, as it was not accessible from the web; d) publication on Twitter took place by obscuring the surname and any other data useful for identification ";

i) with reference to art. 83, par. 2, lett. b) of the Regulations "there can be no doubts about the subjective element in the present case: there was no intention, conscience and will on the part of the Foundation with regard to the events. Where the violation is deemed to have occurred, it assumes the characteristics of slight negligence. In particular, reiterated that the Foundation has not provided any causal contribution to the incident, since this contribution is exclusively and entirely attributable to the Data Processor, there is no culpa in eligendo nor culpa in vigilando ";

j) with reference to art. 83, par. 2, lett. c) of the Regulations, "assuming that the interested parties have suffered damage, the report is immediately followed by a reaction to completely secure the access procedure";

k) with reference to art. 83, par. 2, lett. d) of the Regulations, "the Foundation has for some time equipped itself with a particularly advanced and complete organizational model of privacy management, at the same time taking care of its constant and timely updating thanks also to the support and activity of the DPO. The technical and organizational measures put in place appear adequate in light of the state of the art, the implementation costs, as well as the nature, scope of application, context and purposes of the processing, as well as risks having different probabilities and gravity for the rights and freedoms of natural persons constituted by the processing ";

l) with reference to art. 83, par. 2, lett. e) of the Regulations, "the Foundation has not committed any other violation, this being the first sanctioning procedure in which it is involved";

m) with reference to art. 83, par. 2, lett. f) of the Regulations, "the Foundation immediately sent the relevant report to the Guarantor and promptly responded to every request received, providing all clarifications and making all useful documentation available to the Authority";

n) with reference to art. 83, par. 2, lett. g) of the Regulations, "these are a few single diagnostic frames, absolutely not eloquent and not interpretable in and of themselves even by highly qualified personnel, least of all by ordinary citizens";

o) with reference to art. 83, par. 2, lett. k) of the Regulations, "in the present case it is necessary to highlight the absolute exceptionality, gravity and delicacy of the context in which the Foundation's decision was made and the reasons for this decision. In order to guarantee the safety of the workers, patients and visitors of the Foundation - which is confirmed to be a place of hospitalization and care - the decision was taken to limit access to the facility to non-postponable and strictly necessary cases. In this context, it was necessary to implement a remote access system to diagnostic imaging, in particular in order to allow medical and clinical consultations to be carried out between the treating team and the professional able to correctly interpret these images. Med Store as duly appointed Data Processor guaranteed that this implementation would ensure full compliance with the GDPR. All this to cope with the extremely difficult situation linked to the pandemic spread of the COVID 19 virus; it is emphasized that the Foundation has an obligation to provide curative services but at the same time has an equally binding obligation to ensure health and safety in the workplace for its staff and patients. The aim pursued with the introduction of remote reporting was therefore not linked to profit or interest reasons, but responds to specific obligations

related to the institutional activity carried out by the Foundation and to the protection of an asset, such as health, primary importance ".

The Nursing Home therefore asked to accept the request for filing or, in the alternative, to conclude the procedure with the imposition of a minimal penalty.

3. Outcome of the preliminary investigation.

Preliminarily, it is noted that the data controller can entrust processing "to data processors who present sufficient guarantees to implement adequate technical and organizational measures so that the processing meets the principles of the Regulation", also for the security of the processing, account of the specific risks deriving from the same (articles 28, par. 1, 24 and 32 of the Regulation; see also Cons. no. 81). In this case, "the processing by a manager is governed by a contract or other legal act pursuant to Union or Member State law, which binds the manager to the owner and stipulates the subject matter and the duration of the processing , the nature and purpose of the processing, the type of personal data and the categories of data subjects, the obligations and rights of the owner "(Article 28, par. 3 of the Regulation).

During the investigation it emerged that the installation that allowed the radiologist to view the images to be reported, allowed access to the aforementioned MED Dream software - DICOM viewer designed for diagnosis, viewing, archiving and transmission of medical images usable through a browser web and an access password - on http protocol (hypertext transfer protocol), i.e. a network protocol that does not guarantee the integrity and confidentiality of the data exchanged between the user's browser and the server hosting the service / website and it does not allow users to verify the authenticity of the server they connect to.

In this regard, taking into account the nature of the data being accessed and the high risks deriving from their possible acquisition by third parties, it is believed that the use of the http protocol to access the MED Dream software, as well as the assignment of a user administrative (admin) and non-robust password (admin) to the radiologist, cannot be considered suitable measures to guarantee an adequate level of security (articles 5, par. 1, lett. f), and 32, par. 1, lett. a) of the Regulation, which expressly identifies encryption as one of the possible security measures suitable for guaranteeing a level of security appropriate to the risk; v. also Cons. n. 83 of the Regulation in the part in which it provides that “the data controller […] should assess the risks inherent in the processing and implement measures to limit these risks, such as encryption”; art. 32, par. 1, lett. b) of the Regulation, which establishes that the data controller and data processor must implement measures to "ensure

the confidentiality, integrity, availability and resilience of the processing systems and services on a permanent basis").

The defensive arguments of the nursing home, in relation to the failure to adopt measures for encryption in the transport of data and the absence of checks on the quality of the passwords used for technical users and for users in use by authorized subjects, of measures for the modification compulsory of the same at the first use or, in any case, periodically, as well as automatic blocking mechanisms of the users (in case of repeated unsuccessful access attempts), even if taken into due consideration for the purposes of this provision, are however not sufficient to completely exclude the responsibility of the data controller with regard to the obligations deriving from the regulations regarding the protection of personal data (see articles 24 and 32 of the Regulation).

Although, in fact, during the investigation, the nursing home represented that the aforementioned installation was provided only to meet the need to allow medical personnel, in the context of the emergency context of the pandemic, to view the radiological images to be reported remotely, in order to avoid any possible access to the facility and to protect the health of doctors and patients, it is noted that the configuration for access to the MED Dream software via HTTPS protocol or, in any case, the adaptation in this sense, in the shortest possible period, as well as the creation and assignment of nominal users to the subjects authorized to process the processing, are operations that could have been carried out remotely, even in an emergency context.

The fact that the company Med Store Saronno s.r.l., as Data Processor, guaranteed that the installation of the MED Dream software would allow remote access to diagnostic imaging, ensuring "full compliance with the GDPR", does not exempt from liability the Nursing Home, which should have carried out supervisory, control or revision activities regarding the security of the data processed, on its own behalf, by the Company Med Store Saronno s.r.l.

This, due to the fact that the owner is the subject on whom the decisions regarding the purposes and methods of processing the personal data of the interested parties fall and who has a "general responsibility" on the treatments put in place (articles 4, par. 1, point 7, art. 5, par. 2 of the Regulations - so-called principle of “accountability” and art. 24 of the Regulations); the same is, in fact, required to "put in place adequate and effective measures [and ...] demonstrate the compliance of the processing activities with the [...] Regulation, including the effectiveness of the measures" (Cons. no. 74), also with reference to the preparation of technical and organizational measures that meet the requirements of the Regulation in terms of safety (articles 24 and 32 of the Regulation). This obligation also exists when certain processing operations are carried out by a manager on

his behalf and when he uses products or services made by third parties (see the recent decisions of the Guarantor also relating to the role and related responsibilities of the owner and of the data processor: provision 17 September 2020, nos. 160 and 161, web doc. n. 9461168 and 9461321, provision 11 February 2021, n. 49, web doc. n. 9562852, as well as provision 17 December 2020, 280, 281 and 282, web doc. 9524175, 9525315 and 9525337; see also provision no. 81 of 7 March 2019, web doc. 9121890).

4. Conclusions

From the investigation carried out, it emerges that the technical and organizational measures adopted by the Nursing Home, through the Company Med Store Saronno s.r.l., for the management of access to the aforementioned MED Dream software, with particular reference to the use of the "http "And the methods of assigning the passwords used, are not suitable for guaranteeing a level of security adequate to the risks of the specific processing. Moreover, this contributed to creating the conditions for the occurrence of the violation of personal data, subject to notification, with the consequent unlawful acquisition of personal data, also relating to health, of the interested parties.

For the reasons set out above, contrary to what is claimed in the defensive briefs, the security incident that has occurred cannot be considered attributable only to the Company Med Store Saronno s.r.l., but also to the nursing home, which, too, has made responsible for the failure to adopt adequate technical and organizational measures to guarantee the confidentiality and integrity of personal data processed through the MED Dream software, in violation of articles 5, paragraph 1, lett. f) and 32 of the Regulations.

Therefore, assuming that, unless the fact constitutes a more serious crime, anyone, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces false documents or documents, is liable pursuant to art. 168 of the Code ("False statements to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor"), following the examination of the documentation acquired as well as the statements made to the Authority during the procedure, and in light of the aforementioned assessments, the elements provided by the data controller in the defensive briefs  although worthy of consideration and indicative of the full cooperation of the data controller in order to mitigate the risks of the processing - do not allow to overcome the findings notified by the Office with the act of initiation of the procedure, however, none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the Care Home Foundation Gaetano e

Piera Borghi s.r.l. for having carried out a treatment in violation of the obligations regarding the security of the treatment referred to in art. 32, par. 1, of the Regulation and the basic principles referred to in Article 5, par. 1, lett. f) of the same Regulation.

In this context, considering, in any case, that the conduct has exhausted its effects, the conditions for the adoption of the corrective measures referred to in art. 58, par. 2, of the Regulation.

5. Adoption of the injunction order for the application of the pecuniary administrative sanction and ancillary sanctions (articles 58, par. 2, lett. I and 83 of the Regulation; art. 166, paragraph 7, of the Code).

The violation of articles 5 and 32 of the Regulations, determined by the processing of personal data, the subject of this provision, carried out by the Nursing Home, is subject to the application of a pecuniary administrative sanction pursuant to art. 83, par. 5, lett. a) and par. 4, lett. a) of the Regulations.

Consider that the Guarantor, pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, has the power to "inflict an administrative pecuniary sanction pursuant to Article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, depending on the circumstances of each individual case "and, in this context," the College [of the Guarantor] adopts the injunction order, with which it also disposes with regard to the application of the ancillary administrative sanction of its publication, in whole or in excerpt, on the website of the Guarantor pursuant to Article 166, paragraph 7, of the Code "(Article 16, paragraph 1, of the Guarantor Regulation no. 1/2019).

The aforementioned administrative fine 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 light of the elements provided for in art. 83, par. 2, of the Regulation in relation to which it is noted that:

from the results of the documents, the episode appears to have been isolated and determined by malicious behavior by a third party also detected by the postal police and the negligent liability of the nursing home takes the form of slight negligence (Article 83, paragraph 2, letters a) and b) of the Regulation);

the violation concerned health data but did not affect medical reports, as it involved a single frame of radiological investigation of an interested party and an X-ray relating to another interested party; in addition, the publication on Twitter by hackers took place by obscuring the surname and any other data useful for identification (Article 83, paragraph 2, letters a) and g) of the Regulations);

the nursing home promptly intervened to mitigate the effects of the violation that occurred as well as to prevent the recurrence of similar events, accepting the proposal of the company Medstore Saronno s.r.l. to activate protection in HTTPS (SSL certificate) (Article 83, paragraph 2, letter c) of the Regulation);

the Authority became aware of the event following the notification of personal data breach made, without undue delay, by the data controller himself, who proved to be promptly and extremely cooperative throughout the investigation and procedural phase (Article 83, paragraph 2, letters f) and h) of the Regulation);

no complaints or reports have been received to the Guarantor on the incident, there are no previous relevant violations committed by the data controller, nor have measures previously been ordered pursuant to art. 58 of the Regulations (Article 83, par. 2, letter i) of the Regulations);

the need to implement a remote access system to diagnostic imaging arose in the emergency context of the pandemic from Covid-19, in order to allow medical and clinical consultations to be carried out between the treating team and the professional able to correctly interpret such images, avoiding access on site (Article 83, paragraph 2, letter k) of the Regulation).

Due to the aforementioned elements, assessed as a whole, it is believed to determine the amount of the pecuniary sanction provided for by art. 83, par. 4, lett. a) and par. 5, lett. a) of the Regulations, to the extent of € 30,000.00 (thirty thousand) for the violation of Articles 5 and 32 of the same Regulation as a pecuniary administrative sanction, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary sanction of the publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7, of the Code and art. 16 of the Guarantor Regulation n. 1/2019.

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

WHEREAS, THE GUARANTOR

the violation of articles 5 and 32 of the Regulations, declares the unlawfulness of the processing of personal data carried out by the Gaetano e Piera Borghi Foundation Nursing Home s.r.l. in the terms set out in the motivation;

ORDER

to the Care Home Foundation Gaetano e Piera Borghi s.r.l., with registered office in via Petrarca n. 33, 21020 Brebbia (Va), Tax Code / VAT No. 02779700125, in the person of the pro-tempore legal representative, pursuant to art. 58, par. 2, lett. i) and

83 of the Regulations, as well as art. 166 of the Code, to pay the sum of € 30,000.00 (thirty thousand) as a pecuniary administrative sanction for the violation referred to in this provision; 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 30 days, an amount equal to half of the sanction imposed;

INJUNCES

to the aforementioned nursing home, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 30,000.00 (thirty thousand), according to the methods indicated in the annex, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. . 27 of the law n. 689/1981.

HAS

- the publication of this provision on the website of the Guarantor, pursuant to art. 166, paragraph 7, of the Code;

- the annotation of this provision in the internal register of the Authority - provided for by art. 57, par. 1, lett. u), of the Regulations, as well as by art. 17 of Regulation no. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor - relating to violations and measures adopted in accordance with art. 58, par. 2, of the same Regulation.

Pursuant to art. 78 of the Regulation, of art. 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision, it is possible to 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 applicant resides abroad.

Rome, 2 December 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Cerrina Feroni

THE SECRETARY GENERAL

Mattei