[doc. web n. 9739609]

Injunction order against the Center for Preventive Medicine s.r.l. - December 16, 2021

Record of measures

n. 435 of December 16, 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 dr. Claudio Filippi, Deputy Secretary General;

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 Dr. Agostino Ghiglia;

WHEREAS

1. The violation of personal data.

With a note from the 20th century, the Center for Preventive Medicine s.r.l. (hereinafter "Center") notified the Guarantor,

pursuant to art. 33 of the Regulation, a violation of personal data in relation to a cyber attack attributable to the hacker group "LulzSecita", which resulted in the publication, on the Twitter profile of the same group, of "an image partially obscured in sensitive data (patient name and Patient ID) of a list of names and radio-diagnostic tests carried out on the date of the XX ".

In particular, the Center represented that:

- "a Q / R (Query & Retrieve) was performed on the public IP of the structure and despite the security measures existing at the date of the fact, the hacker group managed to obtain a limited amount of DICOM metadata referable to a list of 5 names of patients who had performed radio-diagnostic tests at the facility on the same day ";
- “the data downloaded from the server are DICOM metadata containing name, surname, date of birth and radiodiagnostic examination performed. No images, no clinical or anamnestic news were downloaded. The image shared by the hackers is obscured in sensitive data and it is highly unlikely to associate that photo with the data involved; (..) the identity of the patients was not made public. However, a regular complaint was filed for the carabinieri ";
- “the" PACS "server is a WINDOWS 10 PC regularly updated and protected by a firewall and is located inside the structure" and the "software that manages the PACS is XX of XX";
- in relation to the technical measures adopted following the violation, "we verified the nature of the attack and verified which and how much data had been downloaded from the server. The data was Dicom metadata from the Pacs XX. We immediately proceeded to change the access ports to the Pacs, all the passwords and tighten the firewall rules. We are considering adding a hardware firewall to the network ”.

2. The preliminary activity.

Following the notification of violation made by the Center, pursuant to art. 33 of the Regulations, the Office asked to provide some useful elements for the evaluation of the profiles regarding the protection of personal data (note of XX, prot. No. XX).

The Center provided feedback with a note from the 20th, stating that:

- "given the small number of subjects involved in the data breach, the company, through the data manager, in the days following the communication to the Guarantor, preferred to contact the subjects by telephone, explaining the nature of the violation, providing information regarding the measures taken to avoid further violations, but above all by recommending maximum attention in case they are contacted by third parties ";
- “on day XX at XX a C-FIND request was made from an IP external to the structure (XX) to the software database XX. A

further request was made at 21:30:32 by another IP (XX), always external to the structure. In response to these two requests, XX sent C-FIND-RSP messages containing the requested information ";

- "given the nature of the two IP addresses (external to the network of the structure), our analysis leads us to affirm that the listening port of the software for receiving DICOM data, despite the fact that at the time of the discovery of the incident it was not reachable from the external, at that moment it was. The aforementioned Netgear D6400 router / modem was updated and password protected (alphanumeric with special characters), but we found that it had vulnerabilities, patched by the parent company only on XX, which probably allowed us to take control of port fowarding ";
- "The logs did not reveal unwanted accesses via the XX web interface. (….), Following the C-FIND-RQ1 request, no other C-MOVE-RQ requests were made, thus indicating that the images were not recovered by the hackers ";
- "In the light of all this, the hackers managed to recover from the database from the software, the metadata of 5 studies containing as many names with relative dates of birth and the type of radio-diagnostic examination performed on the day of the 20th. In the image published by the hackers, these data have been obscured and hardly traceable to the subjects involved; moreover, most of the data in that list do not belong to the structure ".

With regard to the measures taken to remedy the breach of personal data and to mitigate the possible negative effects on the data subjects, the Center stated that "upon discovery of the data breach we immediately verified the nature of the breach and took immediate measures to avoid further unauthorized access. We checked whether there were rules on the router that allowed access to certain ports from the outside, if the firmware was updated and the access password changed. We changed the listening port of the XX software, checked that the security parameters were active and changed all the access passwords of both the server and the software, with the latter having to change at first access. We have also activated an option in the software that allows you to accept requests only from known DICOM devices; an option comparable to a MAC Address filter of a router. In the following days we replaced the router / modem with another more performing model, secure and currently without known vulnerabilities ".

In light of the statements provided, it was necessary to request further elements from the Center and from company XX, concerning the eventual designation of the latter as data processor, pursuant to art. 28 of the Regulation, and the adequate technical and organizational measures put in place to guarantee a level of security adequate to the risk (note of XX, prot. No. XX).

With a note of the XX, the Center declared that “the company XX plays no role with regard to the processing and / or storage of data at our facility. XX is the software house that created the XX software, the PACS system that is used to store and view the radiological images from our facility. The hardware on which it is installed and the storage devices where the data and backup copies are stored were purchased directly from our facility and have nothing to do with XX. Except as provided by the warranty on the software, there is no contract between XX and Centro di Medicina Preventiva Srl. The software was not sold directly by XX to our structure, but by our supplier of radiological equipment. XX was involved in the matter only to analyze the logs and provide the analysis of the violation and verify the extent of the data breach ".

With a note of the XX, the company XX confirmed the declarations of the Center, in relation to the relationship with the latter, also specifying that:

- "in this case, the XX software is installed on hardware made available by the diagnostic center, physically located within the diagnostic center and under the control of the diagnostic center only. This also applies to the storage devices used by the XX software to store and archive digital medical images in DICOM format, as well as to the network devices used for internal communications and for connecting to the Internet ";
- "We do not carry out processing for any reason on behalf of the Data Controller, and, in cases such as the one treated, we are responsible for the connection of our program with the overall computer system of the end user, also for the purposes of matters concerning data transfers and therefore the privacy protection issues concern the installer and the IT manager of the Data Controller ";
- "upon the occurrence of the event, our Company (was) contacted in order to contribute to the analysis of the incident. In summary, it emerged that the vulnus was to be connected to a particular configuration of the router / firewall in use at the diagnostic center for the Internet connection (router / firewall which is under the exclusive control of the diagnostic center responsible for the treatment), which allowed the connection to the DICOM server of XX by IP addresses external to the diagnostic center itself. This made it possible to query the XX archive through a DICOM query request, and to retrieve a series of metadata relating to the exams and patients stored in the archive itself. The analysis also revealed that no diagnostic image was recovered by the hackers ";
- "during this analysis (...), it was NOT necessary to process or even see third party data contained in the IT support, as we limited ourselves to examining portions of log files that contain information on TCP / IP connections and on queries made by

remote DICOM nodes , but no personal data ".

From the "Detailed technical analysis of the hacker attack", carried out by Company XX and transmitted by the same as an attachment to the reply to the Authority's request for information, it emerges that it was not possible "to establish whether that router configuration had been explicitly made by an administrator by mistake or if the hackers exploited a vulnerability of the router to enter the configuration of the same and instantly configure a port forwarding that would allow them access to the DICOM server of XX, TCP port 104; the latter hypothesis, however, appears plausible and is in fact a rather common technique in this type of hacker attacks "(...); if the router / firewall in use at the diagnostic center had not enabled port forwarding on TCP port 104, it would not have been possible to connect to the XX DICOM server from outside the diagnostic center itself. We emphasize that this port forwarding is not absolutely necessary or required even for any remote use of the XX server, for example for remote reporting purposes. The analysis of the log files of XX, which were active at the time of the hacker attack, however, also confirmed that following the interrogation of the metadata relating to the patient's exams, the recovery of the actual diagnostic images was not followed " .

In relation to what emerged during the investigation, the Office, with deed of XX, prot. n. XX, initiated, pursuant to art. 166, paragraph 5, of the Code, a procedure for the adoption of the measures referred to in art. 58, par. 2 of the Regulations, towards the Center, inviting him to produce defensive 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, l. N. 689 of 24 November 1981).

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

- 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). The same provision, in par. 1, lett. b), identifies "the ability to ensure on a permanent basis the confidentiality, integrity, availability and resilience of processing systems and services" as one of the possible measures suitable for guaranteeing a level of security appropriate to the risk (on this point , see also Recital no. 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" that "should ensure an adequate level of security, including confidentiality, taking into account the state of the art and the costs of implementation with respect to the risks that the treatments present and the nature of the personal data to be protected. In assessing the risk for data security, it is appropriate to take into account the risks presented by the processing of personal data , such as accidental or unlawful destruction, loss, modification, disclosure or unauthorized access to personal data transmitted, stored or c anyway processed, which could cause in particular physical, material or immaterial damage ");

- the data controller is required to put in place adequate technical and organizational measures that guarantee, "by default, that personal data are not made accessible to an indefinite number of natural persons without the intervention of the natural person" (art. 25 , paragraph 2, of the Regulation; on this point, see also Recital no. 78 of the Regulation in the part in which it provides that "in the development, design, selection and use of applications, services and products based on the processing of personal data or processing personal data to perform their functions, manufacturers of products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, taking due account of the state of the 'art, to ensure that data controllers and data processors can fulfill their data protection obligations ");

- the data controller, finally, in cases where he is required to designate the data protection officer, is required to publish the contact details of the same and to communicate them to the Supervisory Authority (Article 37, paragraphs 1 and 7 , of the Regulation).

In the same deed, it was also shown that, from the examination of the documentation in the documents, some critical issues relating to the obligations regarding the security of the processing had emerged, with particular reference to the failure to adopt authentication procedures. In fact, at the time the personal data breach occurred, it turned out that the server allowed unauthenticated connections and that it was reachable from the outside. The server, in fact, if properly queried, returned the requested metadata (name, date of birth and type of exam performed) without verifying the identity and authenticating the

subject (man or machine) making the request.

In the aforementioned deed it was therefore highlighted that the solution adopted by the Center could not be considered a suitable technical measure to guarantee an adequate level of security for the risks presented by the processing, considering that the reachability of the server, from the Internet, without authentication, had made it possible for unauthorized parties to access data, including health data.

Furthermore, from a check carried out by the Office, it was found that the Center had not published the contact details of the data protection officer, to be designated pursuant to Article 37, par. 1, lett. c) of the Regulations, and had not communicated them, at the time of verification, to the Guarantor, using the procedure indicated by the same (see "Communication of DPO data - Instructions and facsimile", in www.gpdp.it, doc. web n. 9102796 and "FAQ relating to the telematic procedure for communicating the data of the DPO"); this in violation of art. 37 of the Regulation.

Therefore, the Office had considered that, due to the failure to adopt an authentication procedure, together with the fact that the server was reachable from the internet, at the time the violation of personal data occurred, the Center had carried out a treatment in violation of the obligations referred to in Articles 5, par. 1, lett. f), 25, 32, as well as in relation to the obligations concerning the data protection officer, pursuant to art. 37 of the Regulation.

With a note of the twentieth century, the Center sent its defense briefs, accompanied by specific documentation, in which, in particular, in addition to what has already been represented, it was communicated that:

a) "with regard to the alleged failure to adopt an authentication procedure", according to the report of Strategic Risk Consulting S.r.l. on XX, "instructed by the deductible to shortly conclude the planned remediation activities", it appears that "as regards (..) the vulnerability of the XX, no vulnerabilities have been identified other than those which also exist internally due to the absence of the certificate SSL. The server hosting the application is not reachable from the internet on other ports to query services other than the http one. This means that at the time of the activities it is not possible to extrapolate the information with the methodology indicated by querying port 104 / tcp and from the analysis of the logs available today it is not possible to confirm that the extrapolation actually took place on the server of the Center. Furthermore, given the amount of records published on the LulzSec Italia Twitter page, which is no longer visible today, it is unlikely to imagine that the data were extracted from different clinics and then merged into a single database. On the other hand, having verified that only five names out of the total of 116172 are actually patients of the Center, it would also be possible that those data were brought or shared

with other laboratories actually affected by LulzSec. As for the failure to adopt authentication procedures, it is noted that the same procedure was already configured correctly within the XX application and that the queries that seem to have been made through port 104 / tc are strictly functional to the technology itself as conceived. and put in place during installation; this door is closed to the Internet and cannot be crossed, but in any case it does not release information except of a generic nature and only through an electronic forcing operated by expert IT pirates capable of violating effective protection systems and of proven absolute inviolability, it is not possible confirm that the extrapolation actually took place from the Centre's server ";

b) "with regard to the disputed non-publication of the contact details of the data protection officer, to be designated pursuant to art. 37, par. 1, lett. c) of the Regulations and the failure to notify this Authority, it should be noted that the objection was solved on XX and is to be assessed taking into account the fact that the deductible had delegated every task, including the one in dispute, to her consultant, " In Regola S.r.l. ", necessary in Milan (...), which activated the procedures and defined the organizational and technical rules for the management of company data backups and their restoration, in compliance with the rules of Regulation (EU) 2016/679 (...); (...) the undersigned Center for Preventive Medicine S.r.l. he had relied on that this task had been fulfilled by his consultant and completely unaware of the non-fulfillment, he proceeded to do so without delay as soon as he became aware of it ";

c) "the alleged violation does not appear to be attributable to any intentional or negligent content, nor attributable to the alleged Preventive Medicine Center S.r.l. or to the person in charge of the treatment "; "The same refers only to n. 5 names of patients, did not cause adverse effects on individuals, since no images, clinical or medical history of patients were downloaded and the image shared by the hackers is obscured in sensitive data and it is not possible to associate that photo with the data involved. Therefore the identity of the patients has not been made public ".

The Center therefore asked to accept the request for dismissal of the proceeding. This request was also reiterated with a note of the XX, with which the Center declared that the Strategic Risk Consulting S.r.l., "concluded on the XX the test activities at the deductible and remotely at its technological laboratory started on XX ". To this end, it sent a copy of the report of the aforementioned Company, in which it certifies that "the planned Remediation activities - taking into account the experiences and skills most recently gained following the data breach which affected, as is well known, public bodies (Lazio Region and other Italian Municipalities), as well as international authorities, with very high and unassailable levels of protection - compared to the adequate level of security existing at the time of the assignment (XX), were completed ", specifying that "The system

analyzed therefore presents today an optimal level of security, designed to guarantee the protection of personal data from attempts of unauthorized access or exfiltration, taking into account the state of threats known to date".

3. Outcome of the preliminary investigation.

Preliminarily, it is noted that "personal data" means "any information concerning an identified or identifiable natural person (" interested party ")"; for "data relating to health" "personal data relating to the physical or mental health of a natural person, including the provision of health care, which reveal information relating to his state of health" (art. 4, par. 1, nn. 1 and 15 of the Regulation).

Having said this, having recalled the provisions relating to the obligations of the data controller in terms of security and designation of the Data Protection Officer as well as the principle of integrity and confidentiality of the processing (articles 25, par. 2, 32, 37, and 5 , paragraph 1, letter f) of the Regulation), it should be noted that during the investigation it emerged that, at the time of the violation, the server, if properly interrogated, returned the requested metadata (name, date of birth and type of examination performed) without verifying the identity and authenticating the subject making the request, allowing unauthenticated connections and being reachable from the outside.

Therefore, taking into account the nature of the data being accessed, the object and purpose of the processing, as well as the high risks deriving from their possible acquisition by third parties, it is believed that the solution adopted by the Center cannot be considered a suitable measure. to guarantee an adequate level of security (articles 5, par. 1, letter 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").

On this point, the defensive arguments of the Center do not allow the findings notified by the Office to be overcome with the act of initiating the procedure and are insufficient to allow the filing of the proceedings, however, none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019. This, since the information made accessible (name, surname, date of birth and type of radiodiagnostic examination performed) constitute personal health data that deserve specific protection considering

that, by their nature, they are particularly sensitive, since the context of their processing could create significant risks for fundamental rights and freedoms (Cons. No. 51). Therefore, the same data are subject to particular protection by the Regulation and the fact that, at the time of publication on the Twitter profile of the hacker group, the identification data have been obscured, is not relevant for the purpose of overcoming the finding relating to the accessibility of the aforementioned data.

Furthermore, in relation to the alleged impossibility of confirming that the extrapolation actually took place from the server of the Center, it is noted that this declaration has not been proven and, instead, is refuted by what, on this point, represented by the Center itself. In fact, in the acknowledgment note to the request for information formulated by the Guarantor, the log files of the DICOM server of XX were transmitted, which highlight two requests from IP addresses external to those of the diagnostic center, in response to which XX sent C-FIND-RSP messages containing “the requested information” (“the metadata of 5 studies containing the same number of names with their dates of birth and the type of radio-diagnostic exam”) stored in its archive (see note of XX).

With reference, then, to the obligations relating to the designation of the data protection officer, it should be noted that the data controller, in cases where he is required to designate the data protection officer, must publish the contact details of the same and must also communicate them to the Supervisory Authority (Article 37, paragraphs 1 and 7 of the Regulation). This obligation, in the present case, affects the Center, taking into account that the main activity of the same consists in the processing of particular categories of personal data referred to in art. 9 of the Regulation, which, in consideration of the multiplicity of services offered by the same Center, must be considered to take place on a large scale (see art. 37, par. 1, lett. C) and point 3 of the provision. n. 55 of 7 March 2019, doc. web n. 9091942, relating to the clarifications provided by the Guarantor on the application of the rules for the processing of data relating to health in the health sector). Therefore, in relation to the failure to communicate to the Authority and publication of the contact details of the data protection officer, the fact that the Center had entrusted the burden of implementing the aforementioned obligation to a third party, does not exempt it from liability. , as the same should have carried out supervisory activities and verify the fulfillment of this obligation, due to the fact that the owner has a "general responsibility" on the treatments put in place (see art. 4, par. 1, point 7; Cons. N. 74; 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 "implement adequate and effective measures [and ...] demonstrate the compliance of the processing activities with the [...]

Regulation, including the effectiveness of the measures" (Cons. no. 74),

4. Conclusions

From the investigation carried out, it emerges that the technical and organizational measures adopted by the Center are not suitable for ensuring a level of security adequate to the risks of the specific treatment. 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.

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 declarations made to the Authority during the procedure, confirm the preliminary assessments of the Office and the unlawfulness of the processing of personal data carried out by the Center, in violation of Articles 5, 25, 32 and 37 of the Regulation, within the terms set out in the motivation.

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, 25, 32 and 37 of the Regulations, determined by the processing of personal data, the subject of this provision, carried out by the Center, is subject to the application of a pecuniary administrative sanction pursuant to art. 83, par. 4, lett. a) and par. 5, 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 single 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:

the incident appears to have been isolated and determined by malicious behavior by a third party, reported to the Binasco Station of the Lombardy Carabinieri Legion and the Centre's negligent responsibility takes the form of slight negligence, although it concerned a number in any case not small number of interested parties (Article 83, paragraph 2, letters a) and b) of the Regulations);

the violation concerned health data but did not affect medical reports; in addition, the publication on Twitter by hackers took place by obscuring the surname and any other data useful for identifying the data subjects (Article 83, paragraph 2, letters a) and g) of the Regulations);

failure to adopt suitable security measures to counter any illegal access to servers (Article 83, paragraph 2, letter d), of the Regulation);

the Center promptly intervened to mitigate the effects of the violation that occurred as well as to prevent the repetition of similar events, also by requesting a specific vulnerability assessment and remediation activity from a specialized company (Article 83, paragraph 2, letter c) of Regulation);

the Authority became aware of the event following the notification of personal data breach made, without undue delay, by the same data controller, who proved to be promptly cooperative throughout the preliminary and procedural phase (Article 83, par. 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).

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 € 10,000.00 (ten thousand) for the violation of Articles 5, 25, 32 and 37 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, due to the particular category of data, the

processing of which is the subject of this provision.

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, 25, 32 and 37 of the Regulation, declares the unlawfulness of the processing of personal data carried out by the Center for Preventive Medicine s.r.l. in the terms set out in the motivation;

ORDER

At the Center for Preventive Medicine s.r.l., with registered office in via Amendola 1, 20089, Rozzano (MI), VAT number. 06273780152, 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 € 10,000.00 (ten 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 Center, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 10,000.00 (ten 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, December 16, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Ghiglia

THE DEPUTY SECRETARY GENERAL

Philippi