[doc. web n. 9734934]

Order injunction against Med Store Saronno s.r.l. - December 2, 2021

Record of measures

n. 423 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 Dr. Agostino Ghiglia;

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 ".

2. The preliminary activity.

Following the aforementioned notification, the Office asked the Nursing Home to provide some useful elements for the evaluation of the profiles regarding the protection of personal data (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 the communication received, the Office, with deed of the XXth, 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 Regulations, towards the Company Med Store Saronno S.r.l, (hereinafter the "Company"), 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 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 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 at first use or, in any case, periodically, as well as automatic blocking mechanisms of users in the event of repeated unsuccessful access attempts, 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 has deemed that, at the time when the violation of personal data occurred, the Company Med Store Saronno S.r.l., as data processor , had carried out a treatment in violation of the obligations regarding the security of the 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 company Med Store Saronno s.r.l. sent its defense briefs, in which, in particular, it was represented that:

a) "The Med Store Saronno S.r.l. is a company whose corporate purpose is the wholesale and retail trade of office machines and equipment, computer and peripheral systems, production, development and marketing of commercial, educational, creative application programs and software and hardware consultancy and assistance ";

b) “Med Store is the exclusive distributor for the Italian territory of the MedDream DICOM Viewer software created for the diagnosis, visualization, archiving and transmission of medical images. As a diagnostic image viewer, MedDream consists of a Viewer component, which runs in a browser and does not require any installation on the client device, and a MedDream application server, which manages communication with hospital systems (HIS / RIS / PACS and any other EMR) and prepares the images for streaming to the MedDream DICOM viewer. MedDream uses a flexible and open integration interface for

connection to HIS and / or EMR systems based mainly on URL calls, thus allowing it to be integrated into any medical application ";

c) "Med Store Saronno S.r.l., in relation to the supply to the Gaetano e Piera Borghi S.r.l. Foundation Nursing Home of the software identified above, has been appointed by the same as Data Processor with deed of the XXth ";

d) "on XX, the Foundation requested the Med Store to install the MedDream program to meet the needs deriving from the COVID-19 pandemic emergency which had given rise to the need to allow radiologist technicians to view the images DICOM remotely. At the time of installation, access to the software was guaranteed by a userid and a system password to be associated - during the training period which is usually carried out on site but which could not be carried out due to COVID - to the name of the subject to to which access is guaranteed and to an alphanumeric password chosen by the latter ";

e) "with regard to the nature of the software it is, however, necessary to make a preliminary clarification: MedDream (…) is only a viewer of radiological images. By viewing them it is not possible to access any sensitive data of the patient that detects the state of health. In addition to this, no personal data, other than the name, gender and date of birth can be obtained from accessing the aforementioned software. Furthermore, the MedDream software does not allow data to be saved locally, as all data is deleted when you log out ";

f) "with a telephone call from the twentieth century, the Postal Police informed the Med Store (as the exclusive agent of the Med Dream program and this data being the only one directly obtainable from the tweet in question) of the publication on the Twitter profile @LulzSec_ITA of a tweet containing some sparse images of instrumental diagnostics commented as follows "A lot of money spent in health care, and then our private and sensitive data, are protected by default passwords. How disgusting" with a subsequent tweet of clarification in which this was specified "Guys but no one has said the previous tweet was about San Raffaele. We talk about health in general, that is always a hospital, but not the San Raffaele ";

g) "this Twitter account, suspended in the 20th from the platform but reopened now under a different nickname @LulzSecurityITA, is attributable to the Italian" division "of the Lulz hacker collective, sadly known worldwide for its hacking and disclosure / compromise activities personal data and which, in the COVID era, was characterized by numerous attacks on Italian health facilities for purely emulative purposes ";

h) "in the individual diagnostic images published on Twitter, any reference to tracing the aforementioned images to an identified and / or identifiable person, even indirectly, was obscured by the aforementioned hacker group. In fact, both the

name and the date of birth of the patient were concealed, as well as any element relating to the structure where such diagnostics had been performed ";

i) “immediately, the Med Store was activated in order to support the work of the Postal Police in order to identify the origin of the aforementioned image; This is not an easy task, having only a patient code available. Having identified the origin of the images and immediately replacing the violated password, the Med Store promptly communicated the data from the images to the Postal Police. This was followed by the disclosure of the same to the Foundation and the consequent notification made by the Foundation, the data controller pursuant to art. 33 of the Regulation ";

j) "as a result of this, the Med Store with its e-mail of the twentieth (...) informed the Foundation that, on 25 May at 11.50 am, very fast access had been made in which the individual images were displayed and then posted in the tweet . The Med Store also informed the Foundation that: on the day before and after the improper access, no further access was made by unauthorized persons; the object of access referred only to some single and non-significant images, any access to the clinical study being precluded; the violated passwords had already been replaced ";

k) "the Med Store immediately took a proactive part in identifying corrective mechanisms aimed at better integrating the company network with the aforementioned software, proposing to the Foundation to equip itself with HTTPS protection (SSL certificate), a fulfillment that was promptly implemented in be from the Foundation itself ";

I) "the undersigned Med Store believes that no violation of the obligations regarding the security of processing pursuant to art. 32 of the Regulation and of the basic principles referred to in Article 5 of the same Regulation "as" as regards the use of non-secure network protocols, it means that access to data was the result of an intentional and expert hacking action that involved various subjects carrying out the health care activity and no. The entry into the public IP of the Foundation (...) occurred through the configuration of the non-standard port "88". As is known, this is a well-identified hacker attack by a group that has been involved in such activities for some time and has repeatedly been the subject of judicial authority measures. Moreover, the Med Store - software supplier and responsible for the processing of personal data related to it - is not responsible for the management of the Foundation's corporate network and its security protocols. Notwithstanding the foregoing, immediately and in order to optimize the security systems of the network, the MED Store suggested that the Foundation activate the protection in HTTPS (SSL certificate), associating the public IP address of the Foundation with a web domain and consequently acquiring an SSL certificate for the domain itself. In addition to this, the possibility of interfacing

through LDAP with the password generation system was represented, using the policies already in force by the Foundation. Both of these requirements were subsequently put in place by the Foundation "; "No responsibility on the part of Med Store can therefore be configured from this profile"; "With regard to the failure to define a password policy (...), the Med Store software already complies with the regulatory provisions regarding the quality controls of the passwords used, the measures for the mandatory modification of the same, as well as the automatic locking mechanisms of the utilities ";

m) "what happened is attributable solely to the failure to assign a specific userid and password at the time of installation of the software itself as, (...) for obvious reasons of force majeure; the aforementioned installation took place remotely without having the possibility - for reasons not attributable to Med Store - to carry out on-site training of the subjects in charge of use, also in order to verify the correct access methods to the program ";

n) "access to the public IP of the Foundation did not occur from the standard port 80 but from a NON STANDARD" 88 "port (which denotes the particular expertise of the hacker). Only thanks to this, the authors were able to access the program using the password originally entered and not yet assigned ";

o) "from the installation of the program at the Foundation (remotely) to the hacker attack, only 60 days had elapsed in the period of total Lockdown in which any access to the facility by non-essential health care personnel was precluded";

p) "we reiterate that the MED Dream software is exclusively diagnostic imaging software";

q) "no personal or sensitive data is contained in the image itself, no study or clinical report, no information capable of tracing this image to a particular patient nor to the facility where the diagnostic investigation was carried out. It follows that no material or immaterial damage, not even potential, has occurred in relation to the illegal access in question by the hacker group LulzITA ";

r) with particular reference to the elements for the assessments referred to in art. 83, par. 2 of the Regulation:

in relation to lett. a) "the action (perpetrated by the hacker group) lasted almost instantaneously. There was no access to the software either before or after the illegal entry of the twentieth century. Following the information from the Postal Police, the access credentials were also immediately changed. As already represented by the Foundation and documentally proven by the log files transmitted to it by the writer and by the latter produced to the Authority, the inputs allowed the display of single and sparse diagnostic images (in any way significant) without being any sensitive data accessible "; "In the publication on the Twitter profile of the author of the hacking activity, the hacker group obscured any reference to people or to the structure of the

Foundation itself"; "The installation of the software necessarily took place remotely as any on-site activity was precluded by the COVID legislation in force at the time. Add to this the very short period of time between the installation of the program and the hacking activity in question ";

in relation to lett. b) "excluding for obvious reasons any element of willful misconduct, it is believed that in the present case there can be no responsibility of the person in charge of the processing of personal data even in terms of slight negligence";

in relation to lett. c) “there has been no damage to the parties concerned. From the point of view of third parties, as no personal or sensitive data has been disclosed. On this point, it should be noted, however, that the identification of the image posted on Twitter and its traceability to a patient of the Foundation was extremely complex even for the writer who supplied the software. No damage was caused to the Foundation as access did not lead to any loss, tampering or destruction of data or any reputational damage to the Foundation ";

in relation to lett. d) "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 the risks likely to and different gravity for the rights and freedoms of natural persons constituted by the treatment. These measures, obviously and in terms of on-site training, must be evaluated at the time of the occurrence of the facts and of the lockdown regime in force at the time ";

in relation to lett. f) "The maximum degree of cooperation put in place by the writer towards the Personal Data Processing Manager in reporting the violation and assisting her (...) in relation to all the clarifications requested by the Authority does not appear to be in doubt";

in relation to lett. g) "the alleged violation does not concern" particular "data (referred to in Article 9 of the Regulation) or" relating to criminal convictions and offenses "(referred to in Article 10 of the Regulation). These are (...) single and sparse diagnostic images, not attributable to the person being analyzed or to the structure in which it was carried out and absolutely unsuitable for deriving any information regarding the state of health ";

in relation to lett. h) "The Authority became aware of the violation as a result of the timely notification made by the Owner pursuant to art. 33 of the Regulation ";

in relation to lett. i) "at present there are no corrective measures adopted by the Guarantor to which, if necessary, the writer will comply promptly. With regard to the previous one, please note that, once the unauthorized access was detected, Med Store

immediately activated the replacement of passwords and the (negative) verification of any further access attempts.

Furthermore, although not the specific competence of the writer, the Foundation was advised to adopt the HTTPS protocol with the characteristics described above ";

in relation to lett. k), reference is made to "the pandemic emergency and the lockdown regime in progress at the time of the events".

Therefore, "since the Data Processor is liable for the damage caused by the treatment (damage not verified), only if he has not fulfilled the obligations of the Regulation specifically aimed at the data processors or has acted in a manner different or contrary to the legitimate instructions of the holder of the treatment ", Med Store requested the conclusion of the procedure, by archiving without placing any sanction against it.

3. Outcome of the preliminary investigation.

Preliminarily, it is noted that the data controller can entrust treatment "to data processors who present sufficient guarantees to implement adequate technical and organizational measures so that the treatment meets the principles of the Regulation", also for the security of the treatment, taking into account 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).

Furthermore, although the data controller, who determines the purposes and methods of data processing, has a "general responsibility" for the treatments put in place (see art. 5, par. 2, so-called "accountability", and 24 of the Regulations), even when these are carried out by other subjects "on his behalf" (Cons. no. 81, articles 4, point 8), and 28 of the Regulations), the Regulations governed the obligations and other forms of cooperation to which the data controller is required and the scope of related responsibilities (see articles 30, 32, 33, par. 2, 82 and 83 of the Regulation).

Art. 32 of the Regulation establishes, in fact, that not only the owner, but also the person in charge of the processing, within the scope of his / her competences and the tasks delegated by the owner, "taking into account the state of the art and the costs of implementation, as well as the nature, the object of the context and the purposes of the processing, as well as the risk of varying probability and gravity for the rights and freedoms of individuals "implement" adequate technical and organizational

measures to ensure a level of security appropriate to the risk "And that" 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, in an accidental or illegal way , to personal data transmitted, stored or otherwise processed ".

From the examination of the XXth Nomination Act, it appears that "the assignment is assigned for the following purpose: supply of management software; on-site and remote assistance assistance; software update. The assignment will be responsible for the data present on the following systems: Workstation application software for viewing DICOM images; server: for archiving and viewing WEB images in HTLM 5 ".

That said, it is noted that, 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, display, storage and transmission of medical images usable through a web browser - using 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 / site web and 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 method of accessing the MED Dream software, using the http protocol, cannot be considered a suitable measure. to guarantee an adequate level of security (Article 32, paragraph 1, letter 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 or processor should assess the risks inherent in the processing and implement measures to limit such risks, such as encryption").

In this regard, the statements made by the Company regarding the use of a so-called door cannot be considered relevant. "Non-standard" (88) for the configuration of the http protocol and, in relation to this point, and to the fact that the Company, which would only supply the software, would be responsible for the processing of personal data related to it and not also responsible for managing the corporate network of the nursing home and its safety protocols. This, since, in the state of the art, the use of a non-standard port 88 (instead of the standard one 80) is not a suitable measure to significantly reduce the risks of computer intrusions, given the ease with which it is It is possible to scan a server or host connected to the Internet, even using

tools freely available online, in order to establish which ports it is listening on (port scan) and identify the services running to exploit any vulnerabilities.

The Company, as data processor, should, in any case, have made the configuration for access to the aforementioned MED Dream software using the HTTPS protocol or, in any case, adapt, in the short term and not following the violation, the " installation carried out remotely on the 20th, to allow the radiologist to view the images to be reported, in the growing phase of the COVID-19 pandemic emergency.

During the investigation it also emerged that, 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).

On this point, in relation to the alleged impossibility, declared by the Company, to specifically assign userid and password at the time of installation of the software itself because, "(...) for obvious reasons of force majeure, the aforementioned installation took place remotely without having the possibility - for reasons not attributable to Med Store - to carry out on-site training of the subjects in charge of use also in order to verify the correct access procedures to the program ", it is not proven that the aforementioned assignment could only take place at time of training of the authorized subjects. The need to avoid accessing professionals on-site and the need to provide them, as quickly as possible, with the tools to be able to remotely access diagnostic imaging do not justify the use, by an authorized person, of a technical user with administrative privileges. The creation and assignment of nominal users to the subjects authorized to the processing are in fact operations that could well have been carried out remotely (and not necessarily in the context of a training activity of the subjects to be carried out in presence), even in the emergency context , in a reasonable amount of time (considering that 60 days passed between the software installation and the hacker attack). In fact, after becoming aware of the violation of personal data, the Company replaced the authentication credentials used by the radiologist.

Furthermore, it should be noted that, if a technical user with administrative privileges, such as the one in question, is assigned and used by an authorized subject instead of a nominal user, there could be an inconsistency between the authorization profiles assigned and the actual ones. operational needs, making it possible for this subject to carry out certain processing operations in the absence of a specific intention and instruction from the owner or manager of the processing.

Therefore, even in this case, it is considered that the aforementioned methods of access to the aforementioned software, given the absence of measures for the mandatory modification 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), are not adequate in terms of security, as they do not comply with 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".

4. Conclusions

The Regulation has governed the obligations and specific responsibilities not only of the owner, but also of the data processor, also with regard to the security of the treatment (see articles 32 and 83, paragraph 4, of the Regulation).

From the investigation carried out, it emerges that the technical and organizational measures envisaged and implemented by the Company Med Store Saronno s.r.l., responsible for the treatment of the Nursing Home, for the management of access to the aforementioned MED Dream software, with particular reference to use of non-secure network protocols (http) and the failure to define a password policy, are not suitable for guaranteeing 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 illicit acquisition, by third parties, 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 statements made to the Authority during the procedure, and in light of the aforementioned assessments, the elements provided by the controller in the defense briefs even if worthy of consideration and indicative of the full cooperation of the 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 Company Med Store Saronno s.r.l., as data processor, is noted for the violation of the basic principles referred to in Article 5, par. 1, lett. f) of the Regulations and the obligations regarding the security of processing pursuant to art. 32, par. 1 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 Company, is subject to the application of the 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:

from the findings of the documents, the incident appears to have been isolated and determined by malicious behavior by a third party also detected by the postal police (Article 83, paragraph 2, letter a) and b) of the Regulations);

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 Company promptly intervened to mitigate the effects of the violation that occurred as well as to prevent the repetition of similar events, proposing to the Nursing Home to activate the protection in HTTPS (SSL certificate) and replacing the passwords used (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 (Article 83, paragraph 2, letter f) of the Regulations);

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 € 7,000.00 (seven 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 Company Med Store Saronno s.r.l. in the terms set out in the motivation;

ORDER

to the Company Med Store Saronno s.r.l., with registered office in via Garibaldi 43 at the corner of via Caduti della Liberazione, 21047 Saronno (VA) - VAT / Tax Code 03000070122, 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 7,000.00 (seven thousand) euros 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 Company, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to

pay the sum of € 7,000.00 (seven thousand), according to the methods indicated in the annex, within 30 days from the 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

Ghiglia

THE SECRETARY GENERAL

Mattei