[doc. web n. 9781947]

Order injunction against the Azienda Socio Sanitaria Territoriale Dei Sette Laghi - May 12, 2022

Record of measures

n. 176 of 12 May 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stazione, 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 national law 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 the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46 / EC (hereinafter the "Code");

GIVEN the legislative decree 10 August 2018, n. 101 on "Provisions for the adaptation of national legislation to the provisions of 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 repealing Directive 95/46 / EC ";

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;

HAVING REGARD to the observations made by the Secretary General pursuant to art. 15 of the Guarantor Regulation n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, Doc. web n. 1098801;

Speaker Dr. Agostino Ghiglia;

WHEREAS

1. Violations of personal data

The Azienda Socio Sanitaria Territoriale Dei Sette Laghi (hereinafter the "Company"), on the 20th, notified the Authority, pursuant to art. 33 of the Regulation, a violation of personal data, having as its object the delivery of a digital medium referring to a neuroradiological service to a person who is not entitled to receive it.

In relation to this event, the Company announced that:

"On the XXth date the reporting person goes to the facility, where she carried out a diagnostic test, in order to collect the report. The delivered envelope was correctly headed to the reporting person and also the report inside it concerned the service provided. However, the digital support, inserted in the envelope, referred to another neuroradiological service provided in favor of another subject, causing a loss of confidentiality of the information contained therein. The violation, therefore, is due to the human error of the person who composed the envelope, where he mistakenly entered the digital medium containing the diagnostic test of another person ";

"The Company has procedures and practices aimed at limiting the occurrence of such events. Specifically, all the functions that process patient data must verify the correspondence of the information (name, surname, date of birth and tax code) at the end of each process aimed at archiving, as well as the delivery of documents. In any case, despite (...) the ASST requests the utmost diligence in the management of the documentation from its subjects authorized to process the data, it is not possible to completely exclude the occurrence of human error which, as on this occasion, caused such event";

"The device erroneously delivered to the reporting subject contained the diagnostic test" MRI brain without MDC "";

"The Company in the person of the DPO has taken steps to contact the reporting party in order to obtain the return of the computer device containing the diagnostic test object of the violation, confirming that it will not be accessible to anyone else and that it will be delivered (...) "within a few days," in order to make it available to the legitimate interested party ";

"Have been, and will be in the future, provided training courses in favor of the various company functions that, in carrying out their activities, process personal data, in order to raise awareness on issues relating to data protection and the need to ensure the accuracy of patient information. In any case, a formal warning was sent, aimed at recalling all the personnel involved in the event described with this notification ".

The Company represented that it became aware of the violation as a result of reporting by the person who erroneously received the digital media.

2. The preliminary activity

With regard to the case described, the Office, on the basis of what is represented by the data controller in the act of notification of violation, as well as subsequent assessments, notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of a procedure for the adoption of the measures referred to in art. 58, par. 2, of the Regulations, inviting the aforementioned owner 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, of Law no. . 689 of 11/24/1981). In particular, with deed no. XX of the XX, the Authority held that the Company made a communication of data relating to health in the absence of a suitable legal basis, in violation of the basic principles of treatment and of the obligations regarding the security of treatment (art. 5, par. 1, letter f), 9 and 32 of the Regulation).

The Company has sent its defense briefs, pursuant to art. 166, paragraph 6, of the Code. In particular, with a note of the XX (prot.no.XX), it was declared that:

- "The operational practices in force in the Company provide that the identity of the interested party is subject to multiple checks (i.e. at the time of acceptance, provision of the health service, preparation of the report, delivery of the report)";
- "with specific reference to the paper delivery of medical reports and / or other documentation containing health data, the practices in use, on the date in which the event from which the data breach originated occurred, provided for a double check: the operators health workers involved in the process were called to verify the identity of the interested party (by checking name, surname, date of birth and tax code) both in the preparation of the paper and digital reports and in the envelope phase before proceeding to close the envelope (i.e. the operator, having printed the paper report and prepared the cd / dvd, checked the correspondence of the holders and then placed the two supports in a special named envelope, before proceeding to close it, verified the ownership of the documents included in it);
- "the event involved only one interested party";
- “the violation” has a “culpable nature as it is the consequence of a human error committed by an administrative operator specifically authorized to carry out enveloping operations. More specifically, the operator in charge, having prepared the cd / dvd containing the exam performed and the paper print of the related report, has mistakenly inserted the cd / dvd of another

patient in the envelope containing the paper report of the interested subject, not realizing the mistake made ";

- "The ASST, having become aware of the event, immediately took action in order to re-acquire the digital media erroneously delivered and that the person who erroneously obtained it returned it" and "proceeded to define the roles of the so-called "Corporate privacy organization chart", formally appointing and instructing each of its figures, with particular attention to administrative and health personnel directly involved in the processing of health data ";

- "Having acknowledged that the measures adopted were not sufficient to avoid the occurrence of the event subject to the report (...) the undersigned AAST deemed it necessary to introduce additional control measures. In particular, the operational practice in use has been formalized through insertion in the company quality system and, in order to reduce the risk of committing events similar to the one that occurred, it has provided that the patient is usually only delivered the report in digital format (cd / dvd), without prejudice to the possibility for the interested party (...) to ask the ASST operators to receive a hard copy of the same report ";

- "ASST also provided a specific training course on the subject, highlighting on that occasion the importance of always paying the utmost attention in carrying out the envelope and delivery of reports in light of the serious repercussions that human errors could have on the interested parties. The ASST is also arranging to post special signs in the premises where the reports are delivered, inviting patients to check the correctness of the header of the reports before leaving the hospital ".

3. Outcome of the preliminary investigation

Having taken note of what the Company represented during the procedure, it is noted that:

"personal data" means "any information concerning an identified or identifiable natural person (" data subject ")" and "data relating to health" "personal data relating to the physical or mental health of a natural person, including the performance of health care, which reveal information relating to his state of health "(art. 4, par. 1, nos. 1 and 15 of the Regulation). The latter data deserve greater protection since the context of their processing could create significant risks for fundamental rights and freedoms (Cons. No. 51 of the Regulation);

with particular reference to the question raised, the information on the state of health can only be communicated to the interested party and can be communicated to third parties only on the basis of a suitable legal basis (Article 9 of the Regulation and Article 84 of the Code in conjunction with 'art.22, paragraph 11, legislative decree 10th August 2018, n.101);

the data controller is, in any case, required to comply with the principles of data protection, including that of "integrity and

confidentiality", according to which personal data must be "processed in such a way as to ensure adequate security (…), including the protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage "(Article 5, paragraph 1, letter f) of the Regulation);

regarding the security of the processing, the data controller and the data processor, "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 natural persons (…) implement adequate technical and organizational measures to ensure an adequate level of security for the risk […] "; "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 transmitted, stored or otherwise processed "(art. 32, par. 1 and 2 of the Regulations).

4. Conclusions.

In light of the aforementioned assessments, taking into account the statements made by the data controller during the investigation and considering 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 deeds 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", it is noted that the elements provided by the data controller in the aforementioned defensive brief, although worthy of consideration, do not allow overcome the findings notified by the Office with the aforementioned act of initiating the proceedings, however, none of the cases provided for by art. 11 of the regulation of the Guarantor n. 1/2019.

For these reasons, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by the Azienda Socio Sanitaria Territoriale Dei Sette Laghi is noted, for having communicated personal information, relating to the health of an interested party, to a third party. , in violation of the basic principles of Articles 5, lett. f), 9 and the obligations regarding the security of processing, pursuant to art. 32 of the Regulation.

The violation of the aforementioned provisions makes it applicable, pursuant to art. 58, par. 2, lett. i), the administrative sanction provided for by art. 83, par. 4 and 5 of the Regulation.

In this context, considering, in any case, that the conduct has exhausted its effects and considering that the Company has declared that it has adopted further measures deemed necessary to prevent future similar events, the conditions for the

adoption of measures do not exist, of a prescriptive or inhibitory nature, pursuant to art. 58, par. 2, of the Regulation.

4. 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, par. 1, lett. f), 9 and 32 of the Regulations, caused by the conduct put in place by the Company, is subject to the application of the pecuniary administrative sanction pursuant to art. 83, par. 4 and 5 of the Regulation.

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, for the cases in question, it is noted that:

the Authority became aware of the event following the notification of personal data breach made by the owner and no complaints or reports were received to the Guarantor on the incident (Article 83, paragraph 2, letters h) and k) of the Regulation);

the data processing carried out by the Company concerned data suitable for detecting information on the health of a single data subject (Article 83, paragraph 2, letters a) and g) of the Regulation);

the data controller did not show any intentional attitude, since the violation occurred by mistake in the phase of inserting the CD / DVD of another patient in the envelope containing the paper report of the interested party (Article 83, paragraph 2, letter b) of the Regulation);

the Company has taken charge of the problem by introducing measures aimed at reducing the replicability of the same events that occurred (Article 83, paragraph 2, letter c) of the Regulation);

the owner has demonstrated a high degree of cooperation with the Authority in order to remedy the violation and mitigate its

possible negative effects (Article 83, paragraph 2, letter f) 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 and 5 of the Regulations, to the extent of € 7,000.00 (seven thousand) for the violation of Articles 5, par. 1, lett. f), 9 and 32 of the Regulations, as an administrative pecuniary 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, also in consideration of the type of personal data subject to unlawful processing.

Finally, it is noted that the conditions set out in art. 17 of the regulation of the Guarantor n. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Authority.

WHEREAS, THE GUARANTOR

declares the unlawfulness of the processing of personal data carried out by the Azienda Socio Sanitaria Territoriale Dei Sette Laghi, for the violation of Articles 5, par. 1, lett. f), 9 and 32 of the Regulations, within the terms set out in the motivation.

ORDER

pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, to the Azienda Socio Sanitaria Territoriale Dei Sette Laghi, with registered office in Viale Borri 57 - 21100 Varese, C.F. and VAT number 03510050127, in the person of the pro-tempore legal representative, to pay the sum of 7,000.00 (seven thousand) euros as a pecuniary administrative sanction for the violation indicated 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 Territorial Healthcare Company Dei Sette Laghi, 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 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

pursuant to art. 166, paragraph 7, of the Code, the full publication of this provision on the website of the Guarantor and believes 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.

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 lodge a judicial 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, May 12, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Ghiglia

THE SECRETARY GENERAL

Mattei