SEE ALSO NEWSLETTER OF FEBRUARY 19, 2021

[doc. web no. 9544457]

Injunction against the University Hospital of Siena - 27 January 2021

Register of measures

no. 29 of 27 January 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

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

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

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

Given the documentation in the deeds;

Given the observations made by the Secretary General pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000;

Speaker Dr. Agostino Ghiglia;

WHEREAS

1. The personal data breach.

The Siena University Hospital (hereinafter the Company) has sent the Authority a communication relating to the violation of personal data pursuant to art. 33 of the Regulation, since, "due to a material error in the enveloping phase, third parties

received by post at their residence, a paper medical report referring to other interested parties" (communications of 5 July 2018, prot. n 26398 and of 25.1.2019 - prot. no. 3726, integrated with note 7.2.2019). According to what has been communicated, the Company became aware of this incorrect submission from the subject to whom the aforementioned report relating to a "genetic consultancy" carried out by the UOC of Genetics was erroneously sent. According to what is indicated in the aforementioned communication, this report "does not contain genetic data (no biological sample was taken from the interested parties)", but "data relating to the health and sex life of two natural persons and information on the health of their family members , not identified directly, but "mentioned by relationship".

In this regard, it was also shown that:

- "the paper document erroneously delivered to the reporting third parties was recovered at their residence on 3/10 and on 4/10/2019 delivered to the director of the UOC Medical Genetics";
- "it was intended to change the physical location of the operator responsible for sending medical reports (...) to another more suitable space within the structure to minimize the risk of error";
- "provision was made for the acquisition of a certified department e-mail address for secure sending (...) to replace paper sending where possible and for the generation of specific barcodes for patients".

2. The preliminary investigation.

The Office, with deed n. 36542 of 24 October 2019, with reference to the specific situations of illegality referred to therein, notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in article 58, paragraph 2, of the Regulation, inviting the aforesaid holder to produce defense writings or documents to the Guarantor or to ask to be heard by the Authority (art. 166, paragraphs 6 and 7, of the Code; as well as art. 18, paragraph 1, of law n. 689 of 11/24/1981).

In particular, the Office, in the aforementioned deed, considered that the violation of personal data notified to the Guarantor pursuant to art. 33 of the Regulation, has detected the existence of elements suitable for configuring by the Company the violation of art. 9 of the Regulation, also in the light of the principles of integrity and confidentiality referred to in the deed (art. 5, paragraph 1, letter f) of the Regulation), representing that the conduct described in the notification of violation (sending a medical report, carried out in the context of genetic counseling, containing data on the health and sex life of the data subjects to third parties) supplements a disclosure of health-related data to third parties in the absence of a suitable legal prerequisite.

With a note dated 13 November 2019 (prot. n. 24111), the Company sent its defense briefs, in which, in particular, it was represented that:

- "While waiting to carry out the audit, upon initial verification of the incident, it was ascertained that the medical report of the consultation carried out by Mr and Mrs X/Y had not been sent, as requested in the signed consent, but was archived in the outpatient record. On 27/09/2019 the submission was made. On 09/30/2019 the interested parties were notified by e-mail and on the same date the doctor who had carried out the genetic counseling contacted Ms. Y to clarify what had happened, apologizing and also communicating that he had sent of the medical report. During the phone call, agreements were made on the ways in which the Company could regain possession of the health report not pertaining to them, given the need not to involve further unlawful external subjects and proposing the collection of the medical report by courier specially sent by the Company to whom the document should be delivered, in a sealed envelope, addressed to the Director of the Medical Genetics Unit, the date and time of collection still to be confirmed according to the availability of Messrs. X/Y";
- "On 2/10/2019 the audit was held in the presence of the Clinical Risk Manager, as well as the Director of the Medical Genetics Unit, and other personnel of the same operating unit. During the audit, the Director of the Legal Medicine UOC intervened and the dynamics of the incident were reconstructed, the causes were analyzed and the corrective actions were defined. In particular, it was assumed that instead of their medical report, Messrs X/Y were probably sent a second copy of the medical report referring to two other interested parties, Messrs S/Z";
- "On 10/3/2019, Messrs X/Y delivered, at 18.30, to the courier sent by the Company in a sealed envelope, the medical report received erroneously, which was delivered on 10/4/2019 to the Director UOC Medical Genetics, which was able to ascertain that it was the medical report actually referred, as assumed during the audit, to Messrs. S/Z";
- "Finally, on 10/23/2019, by registered letter (prot. AOUS n. 22273 of 10/23/2019) the Data Controller provided a response to Mr. X/Y to their request dated 9/26/2019 for access to personal data, pursuant to art. 15 of EU Regulation 2016/679, within the deadline of thirty days from receipt of the request itself";
- "The Company immediately recognized the error and the need to acquire all the information useful to circumstantiate the event, limit its potential negative effects, in particular the loss of confidentiality of personal data protected by professional secrecy referring to Messrs. S/Z, whose personal and particular data pursuant to art. 9 of EU Regulation 2016/679 have been - for mere material and involuntary error - disclosed to unauthorized third parties";

- "In addition to fulfilling the obligations required by law in terms of preliminary investigation and full knowledge of the personal data violation, the medical staff of the Medical Genetic Unit contacted the subjects involved (Messrs. X/Y and Messrs. S/Z) at order to disclose the circumstances of what happened, analyze the causes, adopt immediate organizational measures to limit the negative effects and planning the further technical and organizational measures deemed necessary to reduce human error to a minimum";

- "the violation of personal data occurred due to an involuntary material error (error in enveloping the medical report in an envelope bearing the address of residence of a third party) and does not present the characteristics of fraud".

3. Outcome of the preliminary investigation.

Having taken note of what is represented by the Company in the documentation in the deeds and in the defense briefs, it is noted that:

- the regulation on the protection of personal data provides - in the health sector - that 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 prerequisite or on the indication of the interested party same subject to written authorization from the latter (Article 9 of the Regulation and Article 83 of the Code in conjunction with Article 22, paragraph 11, Legislative Decree No. 101 of 10 August 2018; see also general provision of 9 November 2005, which can be consulted on www.gpdt.it, web doc. n. 1191411, deemed compatible with the aforementioned Regulation and with the provisions of decree n. 101/2018; see. art. 22, paragraph 4, of the aforementioned d .lgs. n. 101//2018).

- the Regulation also establishes that personal data must be "processed in such a way as to guarantee adequate security (...), including protection, through appropriate technical and organizational measures, against unauthorized or unlawful processing and against loss, destruction or from accidental damage («integrity and confidentiality»)" (Article 5, paragraph 1, letter f), of the Regulation);

- the sending of a medical report, carried out in the context of genetic counseling, containing data on the health and sexual life of the interested parties, resulted in the communication of the aforementioned data to third parties in the absence of a suitable legal prerequisite.

4. Conclusions.

In the light of the assessments referred to above, taking into account the statements made by the data controller during the

preliminary investigation □ and considering that, unless the fact constitutes a more serious crime, whoever, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances o produces false deeds or documents and is liable pursuant to art. 168 of the Code "False declarations to the Guarantor and interruption of the execution of the duties or the exercise of the powers of the Guarantor" □ the elements provided by the data controller in the defense briefs do not allow to overcome the findings notified by the Office with the deed of initiation of the proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the Siena University Hospital is noted, in the terms set out in the justification, in violation of articles 5 par. 1, lit. f) and 9 of the Regulation.

In this context, considering, in any case, that the conduct has exhausted its effects, given that the Company has declared that the documents erroneously delivered to third parties have been returned and that it has planned the further technical and organizational measures deemed necessary to reduce human error to a minimum, the conditions for the adoption of the corrective measures pursuant to art. 58, par. 2, of the Regulation.

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

The violation of the articles 5, par. 2, lit. f) and 9 of the Regulations, caused by the conduct of the University Hospital of Siena, is subject to the application of the administrative fine pursuant to art. 83, paragraph 5, of the Regulation.

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

The aforementioned pecuniary administrative sanction imposed, depending on the circumstances of each individual case, must be determined in the amount taking into account the principles of effectiveness, proportionality and dissuasiveness, indicated in art. 83, par. 1, of the Regulation, in the light of the elements provided for in art. 85, par. 2, of the Regulation in relation to which it is observed that:

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

the data processing carried out by the Company concerns data suitable for detecting information on the health of a small number of interested parties (Article 4, paragraph 1, no. 15 of the Regulation and Article 83, paragraph 2, letter a) and g ) of the Regulation);

the episode is isolated and characterized by the absence of voluntary elements on the part of the Company in causing the event (Article 83, paragraph 2, letter b) of the Regulation);

the Company immediately demonstrated a high degree of cooperation (Article 83, paragraph 2, letters c), d) and f) of the Regulation).

Based on the aforementioned elements, evaluated as a whole, also taking into account the phase of first application of the sanctioning provisions pursuant to art. 22, paragraph 13, of Legislative Decree lgs. 10/08/2018, no. 101, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 5, letter. a) of the Regulation, to the extent of 10,000 (ten thousand) euros for the violation of articles 5, par. 1, lit. f) and 9 of the Regulation as a pecuniary administrative sanction deemed, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary sanction of publication on the Guarantor's website of this provision should be applied, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Regulation of the Guarantor n. 1/2019, also in consideration of the type of personal data subject to unlawful processing.

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

ALL THIS CONSIDERING THE GUARANTOR

declares the illegality of the processing of personal data carried out by the University Hospital of Siena, for the violation of the art. 5, par. 1, lit. f) and 9 of the Regulation in the terms referred to in the justification.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the Siena University Hospital with registered office in Siena, Strade delle Scotte, 14 – Tax Code/P.IVA 00388300527, in the person of its pro-tempore legal

representative, to pay the sum of 10,000 (ten thousand) euros as of a pecuniary administrative sanction for the violations indicated in this provision, according to the methods indicated in the annex, within 30 days of the notification in the motivation; 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 fine imposed.

ENJOYS

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 10,000 (ten thousand) euros according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of adopting 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 entire publication of this provision on the website of the Guarantor and believes that the conditions set forth in art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

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

Rome, 27 January 2021

PRESIDENT

Station

THE SPEAKER

guille

THE SECRETARY GENERAL

Matthew