[doc. web no. 9561792]

Injunction order against Bergamo hospitals - 11 February 2021

Register of measures

no. 45 of 11 February 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stazione, president, prof.ssa Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and Dr. 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 general secretary pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web no. 1098801;

Speaker Dr. Guido Scorza;

WHEREAS

1. The personal data breach.

The company called Bergamo Hospital Institutes (hereinafter the Company) has sent the Authority a communication relating to

a violation of personal data, pursuant to art. 33 of the Regulation, following the report presented by an interested party in relation to the fact that the latter found, in the digital copy of her medical record, clinical documentation (reports) relating to 7 other patients (communication of 28 December 2019). With reference to the violation communication made by the Company, the data subject filed a report both to the data controller and to the Authority (report dated 12.24.2019).

According to the press release, the Company has advanced the "request for the recovery of the documentation", received erroneously by the reporting party, has launched an "internal investigation aimed at ascertaining and investigating the causes of the incident" and has requested the "review of the procedures relating to the control of the contents of the medical records".

2. The preliminary investigation.

The Office, 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) (note of 5 February 2020, prot. n.4776).

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 the principles of lawfulness, correctness and transparency as well as integrity and confidentiality (Article 5, paragraph 1, letters a) and f) of the Regulation), representing that the conduct (inclusion of third party health documents in the reporting person's medical record) resulted in a communication of data, relating to the health of the interested parties, to third parties in the absence of a suitable legal prerequisite, including the violation of Articles 9 of the Regulation and of the art. 75 of the Code. The Office also considered that the processing of the data in question was carried out with organizational technical measures that were not adequate to guarantee a suitable level of security for the health data processed when the medical records were compiled in digital format, in violation of art. . 32 of the Regulation.

With a note dated 5 March 2020, the Company sent its defense briefs, in which, in particular, it was represented that:

- “Common, personal and contact data (i.e. name, surname, address and date of birth) of the Data Subjects were subject to the Data Breach, as well as data relating to particular categories pursuant to art. 9 of the GDPR, specifically data relating to the health of the Data Subjects. The types of blood chemistry tests conducted on the Subjects concerned were aimed at

highlighting a set of values (including blood count, electrolytes, blood urea nitrogen, blood sugar, creatinine and coagulation) for the sole purpose of performing an anesthesiological evaluation, and not for the purpose of investigating the existence of specific pathologies. In other words, these are standard medical checks aimed at investigating compliance with certain values and/or parameters of the blood samples taken from the Interested Subjects, for the purpose of clinical investigation and organizational forecasting prior to the anesthesiological act for diagnostic and/or therapeutic procedures ";

- "Regarding the duration of the notified violation, finally, it should be noted that the Data Breach occurred when the whistleblower withdrew the copy of the medical record on 6 December 2019, and was detected by the Company following a report made , on behalf of the Whistleblower, by the consumer protection association Adiconsum by registered letter received on 27 December 2019 (advanced by email on 23 December 2019 at 18.02, when the offices are closed). As is known, the Data Breach was subsequently notified to this esteemed Authority on 28 December 2019. In the days immediately following, the undersigned Company proceeded to request the Reporting Party to return the copy of the relative medical record containing the Reports. The return appears to have taken place, after a series of contacts with the whistleblower and according to the times dictated by the latter's needs, on 30 January 2020 at the General Hospital, as per the declaration signed by the whistleblower herself";
- "the Data Breach did not affect any of the whistleblower's personal data. No personal data of the latter, common or belonging to the particular categories referred to in art. 9 of the GDPR, in fact, has been unduly communicated to third parties or disseminated by the undersigned Company";
- "[the Company] sent an internal communication without delay to the offices affected by the Data Breach and to all the operating units, also launching an in-depth internal investigation in order to investigate the causes of the violation and implement the controls carried out on the documents forming part of the medical records";
- "[the Company] has also already undertaken some actions aimed at evaluating the possible areas for improvement of the procedures described and/or of the security systems adopted, including: (i) review, within the Procedure adopted by the Company, of a further check by the medical personnel in charge of the correspondence of all the documentation contained in the medical record; (ii) revision of the procedure by providing for the delivery of laboratory analysis reports relating to gastroenterology directly to the gastroenterology outpatient clinic instead of to the ward; (iii) improvement of the times for entering signed paper reports in the medical record, in order to reduce the amount of documentation in the context of

processing by the personnel in charge of the Procedure".

3. Outcome of the preliminary investigation.

Having acknowledged 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 inclusion in the digital medical record of the signaling health documentation relating to 7 other patients 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 illegality of the processing of personal data carried out by the Bergamo hospitals is noted, in the terms

set out in the justification, in violation of articles 5, 9 and 32 of the Regulation and of the art. 75 of the Code.

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 minimize minimum human error, 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. a) and f), 9 and 32 of the Regulation and of the art. 75 of the Code, caused by the conduct of the Bergamo hospitals, is subject to the application of the administrative fine pursuant to art. 83, par. 4 and 5 of the Regulation, also pursuant to art. 166, paragraph 2 of the Code.

In the present case - also considering the reference contained in the art. 166, paragraph 2, of the Code – the violation of the aforementioned provisions is subject to the application of the same pecuniary administrative sanction provided for by art. 83, par. 5 of the Regulation, which therefore applies to the present case.

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 at the same time as the report received by 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 (7) 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 communication of the data took place in relation to a single person;

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 45,000 (forty-five thousand) euros for the violation of articles 5, par. 1, lit. a) and f), 9 and 32 of the Regulation and of the art. 75 of the Code, as a pecuniary administrative sanction withheld, 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 unlawfulness of the processing of personal data carried out by hospitals in the Bergamo area, due to the violation of art. 5, par. 1, lit. a) and f), 9 and 32 of the Regulation and 75 of the Code in the terms indicated 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 Bergamo hospitals with registered office in Bergamo, Corso Europa, 7 – Tax Code/VAT number 01758140162, in the person of their pro-tempore legal representative, to pay the sum of 45,000 (forty-five thousand) euros as an administrative fine pecuniary for the violations indicated in this provision, according to the methods indicated in the attachment, 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 45,000 (forty-five 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, 11 February 2021

PRESIDENT

station

THE SPEAKER

Zest

THE SECRETARY GENERAL

Matthew