[doc. web no. 9870788]

Injunction order against Eurosanità S.P.A. - December 15, 2022

Register of measures

no. 43/2023

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 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 individuals with regard 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");

HAVING REGARD TO Legislative Decree 10 August 2018, n. 101 containing "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";

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");

HAVING REGARD to 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 on the organization and functioning of the Guarantor's office for the protection of personal data, doc. web no. 1098801;

Supervisor Prof. Geneva Cerrina Feroni;

WHEREAS

1. The complaint, notification of data breach and preliminary investigation

With note of the XX, Mr. XX filed a complaint against Società Eurosanità S.P.A. (hereinafter the "Company"), of which the Policlinico Casilino belongs, in which he stated that he had been contacted by a person having "the same name and surname - Mr. XX, born and resident in another place and with a different date of birth (XX) - who claimed to possess the medical record of P.S." of the same complainant, "erroneously delivered to him and on which he had found the telephone contact, and asked to have his, believing that the same, presumably, had been delivered" to the same complainant. Having gone to the aforementioned health facility, the same Mr. XX learned "at the end of the research carried out by the medical-administrative staff consulted (...) that, in reality, the named homonymous, hospitalized at the P.S. of the Policlinico Casilino in June of the 20th century, did not and had never had a medical record and that, by mistake, the clinical events concerning the latter had been transcribed in the medical record of the (...)" complainant "(admitted for a heart attack in the XX, with a pacemaker implant)".

Following the request for information from the Office (note of the XX, prot. n. XX), with which they were requested, pursuant to art. 157 of the Code, certain information elements useful for the assessment of the case, was provided with a note of the XX, in which it was represented that "Eurosanità S.p.A. following the report received on the XX date, on the XX date it proceeded to make a preliminary notification of a data breach bearing the following number of File XX and Protocol XX. Following the necessary checks, the notification process was concluded on the XX date by making a supplementary notification, bearing the following number of File XX and Protocol XX (...)".

To the XX note, the Company has attached the aforementioned notification of violation of personal data, carried out pursuant to art. 33 of the Regulation and received by the Authority on the XX, as a supplement to the previous notification of the XX.

In the aforementioned notifications it was communicated that:

- the violation took place on the XX;
- "on XX a report was sent to Eurosanità spa by the lawyer of patient XX born in the XX in which he represented that his client on XX was contacted by a third party of the same name who declared that he had been mistakenly given the Emergency Department medical record containing identification data of the patient being assisted. From checks carried out, the date represented above was traced, the XX date of access to the Accident and Emergency Department of the Policlinico Casilino of

patient XX";

- it was an "illegitimate access to personal and particular data (data relating to health) in the event of homonymy. On the XX date, patient XX born in the XX enters the emergency room. The Emergency Room Record is generated erroneously associated with the registry of a patient of the same name born in the XX. Cardiological advice is required during the investigations. The cardiologist checks the hospital management software for any previous accesses by the patient. As a result of the incorrect personal data, the cardiologist records, in the anamnesis, the circumstance of a previous hemodynamic procedure during a hospitalization in the XX (hospitalization actually occurred for patient XX born in the XX). The Emergency Department file of patient XX born in the XX therefore contained personal data that referred to patient XX born in the XX but correctly contained the results of the visits and tests carried out on him. It should be noted that the information relating to the hemodynamic procedure carried out in the XX by XX born in the XX did not in any way influence the diagnostic-therapeutic process";
- "the cause of the violation consists in an accidental internal action (mere clerical error of the personnel assigned to accepting the Emergency Room)";
- "all the staff assigned to accepting the emergency room has been duly authorized and instructed through a specific privacy procedure also attached to the authorization deed. The personnel in charge of the acceptance of the Emergency Department was also trained with a special privacy course and related final test for passing the same";
- the data subject to violation are “personal data, particular data (data relating to health) contained in the Emergency Room medical record. In detail reports, examinations and cardiological consultancy”;
- "only one interested patient is involved and therefore data refer to a single person and only one third party (the aforementioned homonymous born in the twentieth century) has become aware of the personal and particular data of the interested party";
- "the correct personal data of the patient has been restored XX The company that carries out the technical assistance of the regional first aid software has been requested, for further technical measures aimed at reducing the risk of material error by the assigned personnel (such as for example make it compulsory to complete the following personal data fields during the acceptance phase: name, surname, date of birth and the possible activation of a warning that highlights any differences in the data useful for calculating the tax code with those present in the main personal data, by sending an email to technical support).

In addition, the cardiological consultancy on the Emergency Room episode of patient XX born in the XX was also corrected by the referring cardiologist";

- “the need to compulsorily request the Health Card, during the patient acceptance phase, was reiterated to the Emergency Department staff. Only if the patient does not have one can another valid identification document be accepted. The CED will check the master data on a weekly basis to avoid further future similar errors".

2. Assessments of the Department on the treatment carried out and notification of the violation pursuant to art. 166, paragraph 5 of the Code

In relation to the facts described in the complaint and in the violation notifications, the Office, with a note of the XX (prot. n. XX), notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation, inviting you 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 the 11/24/1981).

In particular, the Office, in the aforementioned deed, considered that the Company had carried out data processing in violation of the principle of accuracy, integrity and confidentiality (Article 5, paragraph 1, letters d) and f) of the Regulation) and, through the erroneous drafting of the Emergency Department medical file, subsequently delivered to the homonymous patient of the complainant, communicated health data concerning two patients (the information of the patient born in the XX communicated to the homonymous born in the XX and the information of the patient born in the XX communicated to the homonymous born in the XX) in the absence of a suitable legal prerequisite, in violation of the basic principles of the treatment pursuant to art. 9 of the Regulation and the safety obligations pursuant to art. 32 of the Regulation.

In the same note, the meeting of the proceedings relating to the violation notifications sent, on the XX and XX dates, by the Company to the Authority, pursuant to art. 33 of the Regulation, with that activated by the complaint, considering that they concern the same matter (art. 10, paragraph 4, 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, available on the institutional website www.garanteprivacy.it, web doc. n. 9107633).

With a note of the XX, the Company sent its defense briefs, in which, in particular, in addition to what has already been declared in the previous communications, it highlighted that:

- "the violation was caused by a purely material error of the personnel in charge, adequately instructed and trained by the Data Controller, as required by art. 29 of the GDPR 679/2016 and in compliance with the cardinal principle of Accountability";

- "in fact, the Emergency Room Record was generated erroneously associated with the registry of a patient of the same name born in the 20th century. As a result of the incorrect personal data, the cardiologist recorded, in the anamnesis, the circumstance of a previous hemodynamic procedure during a hospitalization in the XX (hospitalization actually occurred for patient XX born in the XX)";

- "the Emergency Department file of patient XX born in the XX, therefore contained personal data that referred to patient XX born in the XX, but correctly contained the results of the visits and tests carried out on him";

- "it should be noted that the data relating to the hemodynamic procedure carried out in the XX by XX born in the XX did not in any way affect the diagnostic-therapeutic process";

- "only one interested party is involved in the violation (patient XX born in XX). In fact, only one third party, XX born in the XX, has become aware of the personal and particular data of the interested party (XX born in the XX). Furthermore, it is represented that in the present case, data relating to minors as well as the so-called enhanced protection data are not involved";

- "also following specific checks carried out by Eurosanità S.p.A, there is a single communication of data relating to health referable to the information of the patient born in the 20th century to the patient of the same name born in the 20th century and not vice versa. Eurosanità, in fact, has never delivered any medical records to the patient born in the 20th century with data referable to the patient of the 20th century";

- "the Patient born in the XX is, in fact, delivered on the XX date the medical record referable to the access occurred in the XX which correctly reports the data relating to the health referable to him";

- "the violation took place on the date XX" and "is of a negligent nature. The cause of the violation consists in an accidental internal action (mere material error of the personnel assigned to accepting the Emergency Department, even if adequately instructed and trained by the Owner) which generated the Emergency Department Record erroneously associated with the personal details of a patient of the same name. It should be noted that the data relating to the violation and included in the First Aid Card are generated by the Gipse regional first aid software";

- "Eurosanità S.p.A. shows the utmost diligence and cooperation with the Authority, demonstrating good faith and attention

also through the immediate resolution of the problem and the immediate request to the company that carries out the technical assistance of the regional first aid software, further technical measures aimed at reducing the risk of clerical error by the personnel in charge";

- "this is a single communication of data relating to health referable to the information of the patient born in the XX to the patient of the same name born in the XX and not vice versa. In fact, Eurosanità has never delivered any medical records to the patient born in the 20th century with data referable to the patient of the 20th century. The patient born in the 20th has been given the medical record dated 20th attributable to the access that took place in the 20th, which correctly reports the health data attributable to him. (…). Finally, it should be noted that the incident dates back to a time of full health emergency caused by the COVID-19 (XX) pandemic and therefore in a context in which health personnel found themselves operating in highly complex and emergency conditions ".

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:

1. "data relating to health", included among the "particular" categories of personal information, means "personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information relating to his state of health" (art. 4, paragraph 1, no. 1 and 15 of the Regulation; recital no. 35);

2. the data must be "accurate and, if necessary, updated" and "all reasonable measures must be taken to cancel or promptly correct data that are inaccurate with respect to the purposes for which they were processed" (principle of "accuracy"); the data must also be "processed in such a way as to guarantee adequate security (...) including protection, through appropriate technical and organizational measures, against unauthorized or unlawful processing or against accidental loss, destruction or damage" (principle of «integrity and confidentiality») (Article 5, paragraph 1, letters d) and f) of the Regulation);

3. regarding the security of the treatment, the art. 32 of the Regulation establishes that "taking into account the state of the art and implementation costs, as well as the nature, object, context and purposes of the processing, as well as the risk of varying probability and severity for the rights and freedoms of natural persons, the data controller and the data processor implement adequate technical and organizational measures to guarantee a level of security appropriate to the risk [...]" (par. 1) and that "in assessing the adequate level of security particular account is taken of the risks presented by the processing which derive in

particular from the accidental or illegal destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed" (paragraph 2).

4. the regulation on the protection of personal data provides - in the health sector - that information on the state of health can be communicated to third parties on the basis of a suitable legal prerequisite or on the indication of the interested party himself, subject to written authorization from the latter last (art. 9 Regulation and art. 84 of the Code in conjunction with art. 22, paragraph 11, Legislative Decree 10 August 2018, n. 101).

4. Conclusions

In the light of the assessments set out 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 offence, anyone who, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces false deeds or documents, it is liable pursuant to art. 168 of the Code ("False statements to the Guarantor and interruption of the execution of the duties or the exercise of the powers of the Guarantor"), it is noted that the elements provided by the data controller in the defense briefs referred to above are not suitable to allow accepting the requests for dismissal, since the findings notified by the Office with the aforementioned act of initiation of the procedure have not been overcome.

In this regard, in relation to the Company's statement according to which only one patient was involved in the violation, it should be noted that, according to what was declared, it appears that the patient born in the XX, contacted by his namesake, born in the XX, came to knowledge of the information concerning access to the health facility by the same patient born in the XX. Therefore, considering that, in the light of the aforementioned provisions, the news relating to the use of a health service can be included in the category of health data, pursuant to art. 4, par. 1, no. 15 of the Regulation, the subjects affected by the violation are both patients (XX, born in XX and XX born in XX).

In this context, the unlawfulness of the processing of personal data carried out by the Company is noted, in the terms set out in the justification, for the violation of articles 5, par. 1, lit. d) and f), 9 and 32 of the Regulation.

Considering that the conduct has exhausted its effects and that the Company has declared that it has adopted new measures aimed at avoiding the repetition of the complained conduct, the conditions for adopting 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; art. 166, paragraph 7, of the Code).

The violation of the articles 5, par. 1, lit. d) and f), 9 and 32 of the Regulation caused by the conduct of the Company is subject to the application of the administrative fine pursuant to art. 83, par. 4, lit. a) and par. 5, letter. a) of the Regulation.

It should be considered 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 College [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. 83, par. 2 of the Regulation in relation to which it is noted that:

the Authority became aware of the event following a complaint by an interested party and subsequent notification of a violation carried out by the Company, pursuant to art. 33 of the Regulation (art. 83, paragraph 2, letter h) of the Regulation);

the data processing carried out by the Company concerned data suitable for detecting information on the health of two data subjects and resulted in the drafting of incorrect health documentation with potentially serious effects on the health of the data subjects (Article 83, paragraph 2, letter a) and g) of the Regulation);

in terms of the subjective element, no intentional attitude on the part of the data controller emerges (article 83, paragraph 2, letter b) of the Regulation);

the controller has demonstrated a high degree of cooperation with the Authority (Article 83, paragraph 2, letter f) of the Regulation);

a previous provision was adopted against the Company for relevant violations (provision of 21 April 2021, n. 148, web doc. n. 9675228) (art. 83, paragraph 2, letter e) of the Regulation);

the fact occurred in the peculiar emergency context of the Covid-19 pandemic characterized by a high complexity and emergency in which the healthcare personnel found themselves operating (Article 83, paragraph 2, letter k) of the Regulation).

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 4, lit. a) and 5, lett. a) of the Regulation, to the extent of 120,000.00 (one hundred and twenty thousand) euros for the violation of articles 5, 9 and 32 of the Regulation, 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 illegality of the processing of personal data carried out by the company Eurosanità S.P.A. for the violation of the articles 5, 9 and 32 of the Regulation.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to Società Eurosanità S.P.A, with registered office in Piazza dei Caprettari 70 - 00186 Rome, Tax Code/P.Iva: 06726891002, in the person of its pro-tempore legal representative, to pay the sum of 120,000.00 (one hundred and twenty thousand) euros to pecuniary administrative sanction for the violations 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 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 Euro 120,000.00 (one hundred and twenty thousand) according to the methods indicated in the attachment, 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 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, 15 December 2022

PRESIDENT

Station

THE SPEAKER

Cerrina Feroni

THE SECRETARY GENERAL

Matthew