[doc. web no. 9863050]

Injunction against the Bianchi Melacrino Morelli Hospital - 26 January 2023

Register of measures

no. 25 of 26 January 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 movement 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. Reporting and preliminary investigation

With a note dated XX, Mr. XX complained of having received, from the Bianchi Melacrino Morelli Hospital (hereinafter the "Company"), a report relating to a third party, a patient of the same Company.

Following the request for information from this Authority (note of the XX, prot. n. XX, formulated pursuant to article 157 of the Code) with which every element of information useful for the evaluation of the case was requested, the Company has feedback provided, with a note of the XX.

In particular, the Acting Company Health Director pro tempore legal representative, stated that:

- "from what emerged during the internal checks, this procedure, although unauthorized, was activated on the initiative of the Single Withdrawal Center in order to reduce access to the collection desk and offer a service to users. All of this (...), without any knowledge on the part of this Management";
- “more specifically, although with note prot n. XX of the XX (…) the U.O.C. Medical Directorate had given precise indications on the modalities of delivery of the reports, it is represented that: a procedure was in place for delivery of reports, at the request of the interested party, by means of electronic transmission by the operator assigned to delivery of the reports; the online report submission system did not include the measures envisaged by the guidelines in force, nor the security measures envisaged by this Company";
- "from the category of personal data involved in the episode (health data, specifically routine laboratory tests), however, it can reasonably be assumed that no particular consequences have arisen for the data subject";
- “the violation can reasonably be attributed to: non-participation in training activities by the personnel of the Single Withdrawal Center; failure to supervise the work of the operators assigned to the report delivery service";
- "the violation, therefore, seems to be attributable to a lack of supervision, probably related to the chronic shortage of management personnel, further aggravated during the period of the Covid-19 pandemic";
- "the Management, in agreement with the DPO, has undertaken the following actions: immediate suspension of the sending of reports online, with note prot. no. XX of the XX (…); communication to the interested party of the violation, with note prot. XX of the XX (…); communication to the unauthorized third party with request for destruction of the documentation of the interested party, (..) not to use the data, and in any case not to disclose to third parties the health documentation received by mistake,

note prot. no. XX of the XX (…); launch of a cycle of extraordinary training activities to inform all UU.OO directors of the incident, reiterate the ban on sending health documentation by e-mail and highlight the need to fully apply the company security measures - see the notice of convocation of the XX (...) and the attendance register (...); announcement of a public notice for the conferment of the managerial role of Director of the U.0.C. Presidium Medical Directorate, with company resolution no. XX of the XX (…)";

- "also in order to prevent similar violations, moreover, this Company had already previously activated specific measures, such as: annual ECM-accredited training (8 hours), mandatory for all UU.00 Directors/Managers; periodic training (bimonthly) for all privacy representatives; approval of corporate security measures; secure storage; secure exchanges of data and information with other organizations or patients (…); approval of the "Corporate procedure for the correct management of personal data violations" (...); definition of company objectives that take into account the state of application of the GDPR, with the provision of specific audits with all UU.OO. of health area (…); purchase of software dedicated to the delivery of reports in online mode, specifically the purchase of the update of the e-mail service used by Zimbra, in accordance with the provisions of the D.P.C.M. of 8 August 2013, as highlighted by the RPD (note prot. XX of XX). E-mail platform acquired together with the "Citizen's Portal" also for the delivery of reports on the occasion of the renewal of the contract with the soon to be installed supplier (TIM) (determination n. XX of XX) (...); implementation of the "Citizen's Portal" also for the delivery of reports".

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 application, the Office, with a note dated 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 November 24, 1981).

In particular, with the aforementioned deed, the Company was notified of the finding in relation to the processing of data relating to health carried out in the absence of a suitable legal prerequisite, in violation of the basic principles of the processing pursuant to articles 5 and 9 of the Regulation and the safety obligations pursuant to art. 32 of the same Regulation, as well as of the art. 75 of the Code, which is without prejudice to the specific sector provisions contained in the d.P.C.M. August 8, 2013.

With note dated XX, the Company sent its defense briefs, in which, in particular, it highlighted that:

- "it is confirmed that the Great Metropolitan Hospital "Bianchi - Melacrino - Morelli" (G.O.M.) had formalized precise indications on the procedures to be followed for the delivery, exclusively brief manuals of the reports, so that the safety requirements imposed by the regulations protecting the of confidentiality";

- "only from the internal checks carried out after the reporting of the single case object of this proceeding, it emerged that the teller operators, during the maximum period of pandemic emergency, in order to preserve themselves, the continuity of the provision of essential services and the places assigned to the provision of health services resorted to sending reports by e-mail, not systematically, but only at the express request of those directly concerned, moreover in an extremely limited number compared to the daily accesses;"

- "this practice, although contrary to the precise and formal ex post company indications, could be considered understandable if compared to the particular critical moment related to the management of the Covid-19 pandemic. In fact, at the historical moment in which the case in question took place, it was a priority to limit the number of users accessing the hospital premises, both to contain the risk of exposure of healthcare personnel to external sources of contagion, and to contain the User mobility and the spread of the virus. The company management has in fact learned that when a patient undergoing clinical tests requested the sending of the report to their e-mail address to avoid having to go to the hospital again, the operators autonomously adhered to the request, so as to reduce the already high daily presence of patients and their companions";

- "this assessment, carried out on its own by the individual operators, appeared to be not without common sense also considering the particular role of this hospital within the regional hospital network: HUB center and headquarters of the Urgency and Emergency Department - D.E.A. of II Level with a catchment area of about 550,000 inhabitants distributed in n. 97 Municipalities. The services provided in 2019 (the last year of ordinary activity before the Covid-19 emergency) recorded n. 72,634 emergency room accesses, no. 19,860 hospitalizations in the ordinary regime, n. 6,280 day hospitalizations, and no. 723,103 outpatient services. Furthermore, during the pandemic, the G.O.M. it was the only Covid hospital to have to guarantee ordinary hospitalizations for acute cases in the entire province of Reggio Calabria, with the same catchment area described above";

- "the counter operators, who in the period of maximum pandemic emergency have sometimes contravened the rigid and formal company procedures aimed at protecting confidentiality, unfortunately committing, in the present case, a single sending

error, it can be said, without danger of denial, who have acted pursuing the most urgent and important public interest, i.e. the one connected to the containment of the pandemic and the continuity of the provision of the fundamental and irreplaceable health services at the reference hospital for the whole province of Reggio Calabria";

- "with reference to the initiatives undertaken and documented in the first communication of the XX, it is reported that with resolution no. XX of the XX (...) the selection procedure was completed for the assignment of the replacement of the Director of the U.0.C. Presidium Medical Direction. Furthermore, the favorable opinion of the Data Protection Manager was obtained on the implementation of the online collection function of laboratory reports through the "Citizen's Portal" (...), currently in the testing phase".

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. that "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" (Article 4, paragraph 1, no. 15 of the Regulation; recital no. 35); such data deserve greater protection since the context of their processing could create significant risks for fundamental rights and freedoms (recital n. 51);

2. the "data controller" is "the natural or legal person, public authority, service or other body which, individually or together with others, determines the purposes and means of processing personal data" (art. 4, paragraph 1, point 7, of the Regulation);

3. the data controller may provide, under his own responsibility and within his own organizational structure, that specific tasks and functions - connected to the processing of personal data - are attributed to expressly designated natural persons, operating under his own authority. The owner is required to adequately instruct these persons who operate under his direct authority and who have access to personal data, as well as to identify the most appropriate ways to authorize them to process personal data (Article 2-quaterdecies of the Code; see also Article 4, paragraph 1, point 10 and Article 29 of the Regulation);

4. the regulation on the protection of personal data establishes that the same data must be "processed in such a way as to guarantee adequate security (...), including protection, through adequate technical and organizational measures, from unauthorized or illegal processing and from accidental loss, destruction or damage (principle of "integrity and confidentiality")"

(Article 5, paragraph 1, letter f), of the Regulation);

5. the data controller is required to implement "adequate technical and organizational measures to guarantee a level of security appropriate to the risk", taking into account, among other things, "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" (Article 32 of the Regulation);

6. "communication" means "giving knowledge of personal data to one or more specific subjects other than the interested party, the controller's representative in the territory of the European Union, the manager or his representative in the territory of the European Union , by persons authorized, pursuant to article 2-quaterdecies, to process personal data under the direct authority of the owner or manager, in any form, including by making them available, consulting or by interconnection" (art. 2-ter, paragraph 4, letter a), of the Code);

7. the regulations on the protection of personal data provide 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 subject to written authorization of the latter (Article 9 of the Regulation, as well as Article 84 of the Code - in the version preceding the reformulation of the same Code by the legislator with Legislative Decree No. 101 of 10 August 2018 - in conjunction with Article 22, paragraph 11, Legislative Decree No. 101 of 10 August 2018);

8. the online reporting activity is governed by the d.P.C.M. 8 August 2013 containing "Provisions on the methods of delivery by Healthcare Companies of medical reports via the web, certified e-mail and other digital methods, as well as specific security requirements to be adopted in the context of these digital delivery methods" (cf., also, the provision of 19 November 2009 of the Guarantor, published in the Official Gazette No. 288 of 11 December 2009, which can be consulted on www.gpdp.it, web doc. No. 1679033, containing "Guidelines on the subject of online reports" , which continues to apply even after the entry into force of the Regulation, as it is also considered compatible with the same Regulation and with the provisions of decree no. 101/2018; see. art. 22, paragraph 4, of the aforementioned legislative decree .lgs. n. 101/2018); in particular Annex A, point 1.2. lit. b) the aforementioned decree provides, in the context of delivery by e-mail, that the digital report or its electronic copy must be protected with encryption techniques and accessible via a password for opening the file delivered separately to the interested party;

9. in relation to this previous point, the art. 75 of the Code, in summarizing the conditions of the processing of personal data in

the health sector, refers to the need to comply with the specific provisions of the sector.

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 for accepting the requests of archiving, not allowing to overcome the findings notified by the Office with the aforementioned act of initiation of the procedure.

In particular, the fact that the Company was not aware of the practice (albeit contrary to the precise and formal indications of the same) adopted by the branch operators, concerning the sending of reports by e-mail, at the express request of those directly concerned , without taking into account the measures indicated in the aforementioned Annex A of the d.P.C.M. 8 August 2013, does not exonerate the same Company from liability, which should have carried out supervisory, control or auditing activities regarding the security of patient data processing by subjects operating under their direct responsibility. This, due to the fact that the owner is the person responsible for the decisions regarding the purposes and methods of processing the personal data of the interested parties and who has a "general responsibility" for the treatments implemented (Article 4, par. 1, point 7; Article 5, paragraph 2 - so-called principle of "accountability" and Article 24 of the Regulation); the same is, in fact, required to "implement adequate and effective measures [and...] demonstrate the compliance of the processing activities with the [...] Regulation, including the effectiveness of the measures" (recital n. 74), also with reference to the preparation of technical and organizational measures that meet the requirements of the Regulation in terms of safety (articles 24 and 32 of the Regulation).

For these reasons, the illegality 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 the basic principles of the processing pursuant to articles 5, § 1, lett. a) and f) and 9 of the Regulation and the safety obligations pursuant to art. 32 of the same Regulation, as well as of the art. 75 of the Code, which is without prejudice to the specific provisions of the sector including those contained in the d.P.C.M. August 8, 2013.

In this context, considering that the Company has provided suitable assurances by declaring: that it has immediately

suspended "the sending of reports online"; to have sent a request “to the unauthorized third party (…) to destroy the data subject's documentation, not to use the data, and in any case (…) not to disclose to third parties the health documentation received by mistake (…); to have started a "cycle of extraordinary training activities to inform all UU.OO directors of the incident"; to have reiterated "the ban on sending health documentation by e-mail and (...) (highlighted) the need to fully apply the company security measures (...)", 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; art. 166, paragraph 7, of the Code).

The violation of the articles 5, 9 and 32 of the Regulation and of the art. 75 of the Code, 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 (art. 166, paragraph 2, of the Code).

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 observed that:

the Authority became aware of the event following a report from a third party (Article 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 the interested party, a patient of this Company and, in relation to the use of the online method of transmitting reports - which does not comply with sector legislation - of other users who have requested this service (Article 83, paragraph 2, letters a) and g) of

the Regulation);

the controller has demonstrated a high degree of cooperation with the Authority and no measures have previously been taken against the Company for pertinent violations (Article 83, paragraph 2, letters e) and f) of the Regulation);

the Company, in addition to having carried out training courses for the staff, had provided indications regarding the delivery of the reports, to be carried out through the delivery method by hand and the need to use the online reporting method had been put in place by the desk operators in the emergency context of the Covid-19 pandemic, in order to allow interested parties to access their reports, avoiding access to the office; this context also had a further impact on the lack of management personnel for the related supervisory activity (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 and 5 of the Regulation, to the extent of 7,000.00 (seven thousand) euros for the violation of articles 5, 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 the Bianchi Melacrino Morelli Hospital for the violation of articles articles 5, 9 and 32 of the Regulation and of the art. 75 of the Code.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the Azienda Ospedaliera Bianchi Melacrino Morelli Tax Code/P.Iva 01367190806, in the person of its pro-tempore legal representative, to pay the sum of 7,000.00 (seven thousand) euros as an administrative fine for the violations indicated herein measure; 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 7,000.00 (seven 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, 26 January 2023

PRESIDENT

Station

THE SPEAKER

Cerrina Feroni

THE SECRETARY GENERAL

Matthew