[doc. web n. 9583597]

Injunction order against San Giovanni Addolorata Hospital - 11 March 2021

Record of measures

n. 93 of 11 March 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, 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 the national 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 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");

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;

GIVEN 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;

Rapporteur the lawyer Guido Scorza;

WHEREAS

1. Reporting

It was reported to the Authority that a doctor from the San Giovanni Hospital has sent the list of surgeries performed (operating cases), as a medical manager, attached to the application for participation in the public notice adopted by the XX for the

assignment of the management of a complex structure orthopedics and traumatology. In particular, the aforementioned documentation contained personal data, also directly identifying, and on the health of patients (name and surname, hospitalization ward, date and type of intervention carried out).

2. The preliminary activity.

As part of the investigation launched by the Guarantor, an inspection was carried out at the San Giovanni Addolorata hospital (hereinafter the "Company"), aimed at verifying whether access to the information systems had been made on a specific date company by the aforementioned doctor, or another operator, in relation to the interventions carried out by the same.

As part of the aforementioned assessment, carried out on November 5, 2019, it emerged that:

- "The application Log of the application called Sow (Web Operating Rooms), used at the time of the facts and in the discontinued state, recorded the user login and logout. In addition to these logs, the system allowed to record the Selections made by users. These system logs are not kept at the moment, as the log data recorded in backup have been overwritten ";
- "the application currently in use in the operating room is called B.O. (Operating Block), which allows for the extraction of data relating to subjects who perform the surgery, divided by department. On the B.O. the logs of the operations carried out are tracked. These logs are stored in a recording system that detects the last 10 historical logs plus the online one, for a maximum capacity of 10 Mega. From the assessment carried out, the last 10 logs are recorded, which date back to the last 30 minutes of system operation. Currently from the B.O. it is not possible to access the data recorded on the Sow system "(see report of the operations carried out).

With a note dated November 22, 2019, the Company intended to specify that:

- "is strengthening its policy of monitoring the accesses made by certified users, to all applications in use, by immediately extending the time horizon for storing log files";
- "in this direction, the Entity has already concretely initiated specific actions to optimize storage capacity, as well as improve the system for registering access to company applications. In particular, the log management system for accessing the application logs of the AREAS clinical health platform (BO, ADT, Clinical record, Pre-hospitalization record, etc.) was reconfigured, allowing them to be completely logged and displayed ";
- “the comparison of the safety and protection profiles of the information systems will allow to monitor, with greater efficiency, the access procedure and the exit procedure from the applications of each recognized user”.

In light of the findings, the Office, with act no. 37494 of 9 October 2020, 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, 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, the Office, in the aforementioned deed, represented that, on the basis of the elements acquired, it appeared that the Company had carried out a processing of personal data, in violation of the provisions regarding the security of processing, by Articles 5, par. 1, lett. f) and 32 of the Regulation, as it was verified that, as of 5 November 2019, the log files relating to the access operations to the B.O. (Operating Block) which allows for the extraction of data relating to patients undergoing surgery were kept for a period of time insufficient to guarantee the security of the data, equal to about 30 minutes, corresponding to the recording of the last 10 accesses. in the system.

In this regard, it should be borne in mind that the Guarantor, in relation to the traceability of accesses, with reference to the health record, had highlighted that "the owner must identify an appropriate retention period for the operation tracking logs that responds, on the one hand, to need for interested parties to become aware of the access to their personal data and the reasons that determined it and, on the other hand, to the legal medical needs of the healthcare facility that is the owner of the processing of personal data ", identifying, as appropriate, a retention period of not less than 24 months from the date of registration of the operation (see provision containing the "Guidelines on Health Dossier", of 4 June 2015, published in Official Gazette 164 of 17 July 2015, available on www.gpdp. it, web doc. no. 4084632).

With a note dated November 6, 2020, the Company sent its defense briefs, in which it was represented that:

- “specifically and with reference to the concrete initiatives put in place (…)” it should be noted “that on 27 May 2020, after in-depth technical analyzes and exhaustive discussions with the IT service provider, resolution number 420 / D.G. concerning the services of Virtualization of databases and Management of the virtual infrastructure and the supply of Hardware for the upgrading of the infrastructure itself needed by the Hospital ... ";
- "this substantial resolution goes in the direction of expanding the control and maintenance services of the systems, specifically the virtualization of the Data Base, the HW enhancement and the management of the virtual infrastructure, in order to meet the changed needs and criticalities that have also emerged in following the activity of this Authority ".

Subsequently, with a note dated January 27, 2021, the Company integrated the aforementioned briefs, producing further

defensive writings, in which what had already been highlighted in the note of November 22, 2019, in relation to the actions initiated immediately after the inspection activity was reiterated. carried out by the Authority, specifying that:

in November 2019, in the reconfiguration of the log file management system for accessing the applications of the aforementioned clinical health platform, "the complete historicization and display of the same was envisaged, with a duration of the log files set at 18 months (from November 2019) ";

in May 2020, new hardware and new software were purchased and an "enhancement of the Data Base Virtualization and Virtual Infrastructure Management services and the supply of Hardware for upgrading the infrastructure were carried out (...). These new services confirm what was already highlighted in November 2019, but with better technical performance ".

3. Outcome of the preliminary investigation.

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

1. the Regulation provides that personal data must be "processed in such a way as to guarantee adequate security (...), including protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from loss, destruction or accidental damage ("integrity and confidentiality") "(Article 5, paragraph 1, letter f) of the Regulation). The adequacy of these measures must be assessed by the owner and the processor with respect to the nature of the data, the object, the purposes of the processing and the risk for the fundamental rights and freedoms of the data subjects, taking into account the risks that derive from destruction, loss, modification, unauthorized disclosure or access to personal data (Article 32, paragraphs 1 and 2 of the Regulation);

2. with specific reference to the management of health dossiers, the Guarantor adopted the aforementioned provision of 4 June 2015, which continues to apply even after the Regulation has come into force, as it is considered compatible with the same Regulation and with the provisions of decree no. 101/2018 (see article 22, paragraph 4, of the aforementioned legislative decree no. 101/2018);

3. in the aforementioned Guidelines, the Guarantor has provided, in terms of data security, the traceability of accesses and operations carried out, highlighting, in particular, that "the health structures, within the scope of the discretion recognized in organizing the compliance, must implement control systems for the operations carried out on the health record, through procedures that provide for automatic registration in specific log files of accesses and operations performed. In particular, the

log files must record for each access operation to the dossier carried out by an appointee, at least the following information: the identification code of the person in charge who carried out the access operation; the date and time of execution; the code of the workstation used; the identification of the patient whose dossier is affected by the access operation by the person in charge and the type of operation performed on the data. Due to the particular delicacy of the processing of personal data carried out through the dossier, it is also necessary to trace the operations of simple consultation (inquiry) "; it was also provided that "the owner must identify an appropriate retention period for the transaction tracking logs that responds, on the one hand, to the need for interested parties to become aware of the access to their personal data and reasons that determined it and, on the other hand, to the medical-legal needs of the healthcare facility that is the owner of the processing of personal data ", evaluating a retention period of not less than 24 months from the date of registration of the operation as appropriate;

4. although the aforementioned indication regarding the storage time of the log files refers to the health record (and not also to individual applications), it had to be taken into consideration by the owner for the purpose of identifying an appropriate period storage of log files of accesses to the application that manages the information system of the operating room, called B.O .;

5. from the point of view, then, of determining the applicable legislation, from a temporal point of view, the principle of legality referred to in art. 1, paragraph 2, of the l. n. 689/1981, which states that "the laws that provide for administrative sanctions are applied only in the cases and times considered in them". This determines the obligation to take into consideration the provisions in force at the time of the committed violation, which in the case covered by this provision - given the permanent nature of the alleged offense - must be identified at a later date than 25 May 2018, in to which the Regulation has become applicable. In fact, during the inspection carried out, it was verified that, as of 5 November 2019, the access tracing log files were kept for an inadequate period, equal to about 30 minutes, corresponding to the registration of the last 10 accesses about in the system.

4. Conclusions.

In the light of the aforementioned assessments, taking into account the statements made by the data controller during the investigation and inspection 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, and is liable pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the tasks or 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 initiation of the procedure, however, as none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the San Giovanni Addolorata Hospital in the terms set out in the motivation, for violation of Articles 5, par. 1, lett. f), and 32 of the Regulation.

In this context, considering, in any case, that the conduct has exhausted its effects, the conditions for the adoption of the corrective measures referred to in art. 58, par. 2, of the Regulation.

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

It should be considered 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. 85, par. 2, of the Regulation in relation to which the temporal duration of the violation is taken into account (approximately 18 months), the fact that the data processing carried out by the Company concerns data suitable for detecting information on the health of numerous patients, the absence of elements of voluntariness on the part of the Company in the cause of the event, of the degree of responsibility of the Company, of the cooperation of the same, also during the inspection (art.83, par. 2, lett. a), b), d ), f), g) 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, lett. a) and par. 5, lett. a) of the Regulations, to the extent of € 20,000.00 (twenty thousand) for

the violation of Articles 5, par. 1, lett. f) and 32 of the Regulations as a pecuniary administrative 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 potential number of interested parties and the type of personal data subject to unlawful processing.

Finally, it is noted 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.

WHEREAS, THE GUARANTOR

declares the unlawfulness of the processing of personal data carried out by the San Giovanni Addolorata Hospital, for the violation of Articles 5, par. 2, lett. f) and 32 of the Regulations in 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 San Giovanni Addolorata Hospital with registered office in Rome, Via dell'Amba Aradam 9, - Tax Code / VAT No. 04735061006, in the person of the pro-tempore legal representative, to pay the sum of € 20,000.00 (twenty thousand) as a pecuniary administrative sanction for the violations indicated in this provision, according to the methods indicated in the annex, within 30 days from the notification of 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 sanction imposed.

INJUNCES

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 € 20,000.00 (twenty 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

- the publication of this provision on the website of the Guarantor, pursuant to art. 166, paragraph 7, of the Code;
- the annotation of this provision in the internal register of the Authority - provided for by art. 57, par. 1, lett. u), of the Regulations, as well as by 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 - relating to violations and measures adopted in

accordance with art. 58, par. 2, of the same Regulation.

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 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, March 11, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei