[doc. web n. 9689566]

Injunction order against the Bambino Gesù Pediatric Hospital - June 24, 2021

Record of measures

n. 250 of 24 June 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, Prof. 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 Code regarding the protection of personal data, containing provisions for the adaptation of national law to regulation (EU) 2016/679 (Legislative Decree 30 June 2003, n.196, as amended by Legislative Decree 10 August 2018, no. 101, hereinafter the "Code");

GIVEN the 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, relating to the protection of individuals with regard to the processing of personal data, as well as the circulation of such data and repealing Directive 95/46 / EC (General Data Protection Regulation);

HAVING REGARD to the "Guidelines on Health Dossier - 4 June 2015" (Provision 4 June 2015, published in Official Gazette 164 of 17 July 2015, web doc. No. 4084632);

HAVING REGARD to the “Guidelines 01/2021 on Examples regarding Data Breach Notification” adopted by the European Data Protection Committee on 14 January 2021;

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");

Having seen the documentation in the deeds;

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

Speaker Dr. Agostino Ghiglia:

WHEREAS

1. The breach of personal data.

On 10 March 2020, the Bambino Gesù Pediatric Hospital in Rome (hereinafter OPBG), as the data controller, notified the Guarantor, pursuant to art. 33 of the Regulations, a violation of personal data "following a report by the parent of a patient (minor) who requested the updating of the printing of the documentation of interest as it contained data referring to another patient".

In the aforementioned notification, the Hospital stated, in particular, that "the violation concerned the printing service of the medical record for subsequent delivery to the patient through the" health card "tool or shipping to home. The printing process, due to a bug that considered only the episode number while neglecting the patient code, also presented another patient's first aid file. The bug was not found because the display of the folder from the repository was correct and the printing is produced by an automatic tool; for reasons of confidentiality, the staff who produce the prints, not being authorized, do not consult the content but send the file to be archived and published. The violation involved a total of 19 folders of which 17 were sent to the patient by post and 2 consulted through the "health card" ".

In the act of notification, the OPBG specified that the violation occurred in the period between January 14 and February 13, 2020 and to have become aware of it, on March 5, 2020, following "the information to the Data Controller by the Head of the Hospital's Privacy Function who, together with the DPO, coordinated the functional investigation for the analysis of the accident that occurred ", launched following receipt of the aforementioned report.

2. The preliminary activity.

With reference to the aforementioned violation, with a note dated 26 March 2020 (prot. No. 12145), the Office requested information from the OPBG regarding the technical-organizational causes that led to the violation of personal data.

With a note dated 10 April 2020 (prot. No. 885), the OPBG, in providing a response to the aforementioned request for information from the Office, represented that:

"The subject involved in the processing of personal data subject to violation is the XX by virtue of the contract for the supply of the medical record management system and relative appointment as Manager pursuant to art. 28 ";

"First aid episodes have a progressive numbering independent and different from that of hospitalizations, although they have the same 'year + progressive" format; however at the beginning of the year, when the progressive is initialized, the two numbers, for a short period of time, they travel with similar numbers. The printing program that produces the patient documentation (including the first aid report and electronic medical record) has revealed a structural malfunction for which the pair of "patient code" indexes was not considered and "episode number", but only (...) the episode number. This malfunction meant that, for some patients, the documentation contained the electronic medical record to each of them correctly referred to, while the report was associated with each record emergency room of another patient, this is because the events had the same number but of a different series a violation ";

to have provided "as soon as evidence of the situation" interrupted the union of the documents of the different episodes; Identification of patients with documentation presenting the problem; Cancellation of documentation not correctly associated with the patient from the health card; Identification of patients to whom the documentation in paper format had been sent or who had already consulted the documentation itself through the health card; Sending of the correct documentation with an accompanying communication as follows: "Dear Mr. From an internal control we have ascertained the occurrence of a computer error that caused the transmission to you of the medical record no. Containing irrelevant health documentation. We apologize for the 'happened, we send you the document again and we kindly ask you to destroy the one received previously. We remind you that any modification or distribution to third parties is absolutely forbidden. We also remind you that the communication, dissemination, use and / or storage of the data received in error, constitute violations of the provisions of the General Regulation on the protection of personal data 679/2016 of the European Union and are punishable "".

the "request for correction of the program (...) was sent to the supplier, and a report was requested on the incident";

"As for the correction of the bug, (...) it is being resolved, while, in the meantime, the inclusion in the medical record of non-hospitalization reports has been interrupted (...) now an activity is underway to introduce a new file archiving function, for use by healthcare personnel, which generates the pdf file and which can therefore be checked by authorized personnel before being sent to patients or to the health card ".

In relation to what emerged from the documentation, the Office notified the OPBG, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in art. 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) (note of October 20, 2020, prot. No. 38986).

In particular, the Office, in the aforementioned deed, found the existence of elements suitable to configure by the OPBG the violations of the basic principles applicable to the treatment referred to in art. 5, par. 2, lett. f) and art. 32 of the Regulation.

In producing its defense writings, the OPBG reiterated everything already represented to the Authority in the preliminary investigation phase, providing some specific additional elements aimed at substantiating the violation that occurred and allowing the Authority to make a weighted assessment of the same pursuant to art. 83 of the Regulation (see note of November 19, 2020, prot. N. 2244 / PR).

With this deed, the OPBG specified, in particular, that:

the anomaly in question would have materialized in the production of prints that had attached the emergency room report of other patients because "it was found that the printing program worked only on the episode number, ignoring the patient's code. The printing program that produces the patient documentation (including the first aid report and electronic medical record) revealed a structural malfunction for which the pair of indexes "patient code" and "episode number" was not considered. Because of this anomaly, hospitalizations and first aid episodes that had the same code but were from different patients were merged ”.

"The Hospital did not have prior evidence of the anomaly, since the folder viewed from the repository by health personnel did not show this problem, while the print is produced with a tool of the company XX, therefore, the files are sent for publication without the prior consultation of the information systems staff, whose technical staff does not check the content of the .pdf file in compliance with organizational measures that aim to protect the particular data of patients ";

"This error, therefore, was not foreseeable, because by accessing the legal repository of wHospital, where all the patient's clinical documentation is present (...), there were no reports that appeared by mistake in the press";

“In relation to the bug in question, therefore, it is appropriate to highlight how this is configured as a logic bug of the“ PRINT FOLDER ”function;

"In any case, it should be noted that the reporting to the system Supplier has been made, the same has made the necessary corrections and the checks carried out, both in the test and production environment, have confirmed that unauthorized access to the user data. Furthermore, as a greater guarantee for the interested parties, a different method of inserting the file filing has

been introduced, carried out by the healthcare staff who generates the pdf file, and which therefore places an additional level of control, by the authorized staff, before the sending to patients or to the "health card";

"The subjects to whom the information was disclosed, due to the bug described, were a limited number and (...) the event that occurred, in the light of what has been illustrated, did not have any effect on a significant number of interested parties and for a very limited period of time ";

"The Hospital could not have previously noticed this anomaly since it would have occurred only when the medical records are printed and this print is produced with a tool developed by the XX, therefore, the files are sent for publication without prior consultation of the information systems personnel, whose technical personnel do not check the contents of the .pdf file in compliance with organizational measures that aim to protect the particular data of patients ".

The data controller also highlighted that in 2020, with the support of the data protection officer, it implemented a new risk management system which has the priority objective of monitoring corporate risks ex ante and implementing effective measures to reduce the probability of unwanted events occurring.

3. Outcome of the preliminary investigation.

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

- the processing of personal data must take place in compliance with the applicable legislation on the protection of personal data and, in particular, with the provisions of the Regulation and the Code;

- with particular reference to the question raised, it is pointed out that personal data must be "processed in a lawful, correct and transparent manner" (principle of "lawfulness, correctness and transparency") and "in such a way as to guarantee adequate security (...), including the protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage (principle of "integrity and confidentiality") "(art. 5, par. 1, lett. a) and f) of the Regulation). It is also stated that the data must be "accurate and, if necessary, updated", "all reasonable measures must be taken to promptly delete or rectify inaccurate data with respect to the purposes for which they are processed (" accuracy ") (subsequent letter d));

- the Regulation then provides that the data controller implements "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

purpose of the processing, as well as the risk of varying probability and gravity for the rights and freedoms of natural persons "(Article 32 of the Regulation). The Regulation also provides that, "in assessing the adequate level of security, special account is taken of the risks presented by the processing that derive in particular from the destruction, loss, modification, unauthorized disclosure or access, in accidental or illegal way, to personal data transmitted, stored or otherwise processed "(art. 32, par. 2);

- in this regard, it should be noted that, in any case, the data controller is required to adopt procedures "to test, verify and regularly evaluate the effectiveness of technical and organizational measures in order to guarantee the security of treatment" (Article 32 , paragraph 1, letter d));

- with specific reference to the facts that are the subject of the aforementioned notification, it should also be noted that the Guarantor has adopted the "Guidelines on the health dossier - June 4, 2015" (Provision of June 4, 2015, published in Official Gazette 164 of July 17, 2015 , web doc. no. 4084632), in which an initial framework of caution has been identified, in order to outline specific guarantees and responsibilities, as well as necessary and appropriate measures and precautions to be put as a guarantee for citizens, in relation to the processing of health data that concern them;

- in the aforementioned Guidelines, the Authority highlighted the need to ensure certainty about the origin of the data processed, its accuracy, integrity and non-modifiability, as well as its availability (point 7, Annex A to the Guidelines);

- on the basis of the elements acquired and the documentation on file, it is ascertained that due to a bug in the printing process of the documents present in the "health card", or in the hospital health dossier, the health documentation of 19 interested parties has been made available unauthorized;

- the "GENERATE PRINT" function of the wHospital support program has not been subject to testing and inspection by the Hospital.

4. Conclusions.

In light of the aforementioned assessments, taking into account the statements made by the owner during the investigation □ 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 o 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 OPBG of Rome, under the terms set out in the motivation, is found, in violation of Articles 5, par. 2, lett. f) and 32 of the Regulations.

In this context, considering, in any case, that the conduct has exhausted its effects, given that the Hospital has declared:

to have provided for the inhibition of the printing function of the merging of documents and to have proceeded with the identification of patients whose medical records contained third party data, the deletion of third party data from patient records and the sending of the correct documentation to patients with instructions to destroy the previous incorrect one (see note of 10 March 2020).

with regard to the security measures taken to prevent similar personal data breaches in the future, to have requested the external provider XX, to modify the program used to eliminate the bug and to insert in the press the episodes per patient, and to have adopted as a measure organizational verification, by personnel authorized for consultation, of the print before delivery to the patient (see note of 10 March 2020),

to have carried out specific training of personnel in the field of personal data protection.

Therefore, 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. 2, lett. f) and 32 of the Regulations, caused by the conduct put in place by the Bambino Gesù Pediatric Hospital, is subject to the application of a pecuniary administrative sanction pursuant to, respectively, art. 83, par. 5, lett. a) and par. 4, 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 it is noted that:

the Authority became aware of the event following the notification of personal data breach made by the same owner 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 processing of data carried out by the Hospital concerns data suitable for detecting information on the health of a limited number of interested parties (Article 4, paragraph 1, No. 15 of the Regulation and Article 83, paragraph 2, letter a) and g ) of the Regulations);

the episode is characterized by the absence of voluntary elements on the part of the hospital in the cause of the event (Article 83, paragraph 2, letter b) of the Regulations);

the OPBG immediately implemented measures aimed at mitigating the damage suffered by the interested parties (Article 83, paragraph 2, letter c) and d) of the Regulations);

the Hospital immediately demonstrated a high degree of cooperation (Article 83, paragraph 2, letters c), d) and f) of the Regulations);

the OPBG is the recipient of a warning for the violation of the same regulatory provisions even if applied in relation to treatments carried out for scientific research purposes (provision of 17 September 2020, web doc. 9479364).

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. 5, lett. a) of the Regulations, to the extent of € 15,000 (fifteen 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 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 Bambino Gesù Pediatric Hospital, for the

violation of art. 5, par. 1, 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, from the Bambino Gesù Pediatric Hospital, with registered office in Piazza S. Onofrio n. 4 - 00165 Rome Tax Code 80403930581, in the person of the pro-tempore legal representative, to pay the sum of € 15,000 (fifteen 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 hospital, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 15,000 (fifteen 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

pursuant to art. 166, paragraph 7, of the Code, the full publication of this provision on the website of the Guarantor and believes 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.

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, June 24, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Ghiglia

THE SECRETARY GENERAL

Mattei