[doc. web no. 9542155]

Injunction against the Local Health Authority of Bologna - 14 January 2021

Register of measures

no. 11 of 14 January 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, 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 natural persons with regard to the processing of personal data, as well as to the free movement of such data and which repeals Directive 95/46/EC (hereinafter the "Code");

CONSIDERING the Regulation n. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved with resolution no. 98 of 4/4/2019, published in the Official Gazette no. 106 of 8/5/2019 and in www.gpdp.it, doc. web no. 9107633 (hereinafter "Regulation of the Guarantor n. 1/2019");

HAVING REGARD to the documentation in the deeds;

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

Speaker Prof. Pasquale Stanzione;

WHEREAS

1. The personal data breach.

The Local Health Authority of Bologna (hereinafter Company) has notified the Guarantor of a violation of personal data pursuant to art. 33 of the Regulation in relation to the report made on 29 August 2018 by the Oncology department of the

Bellaria Hospital regarding the complaints made by two patients in relation to the presence, on their EHR, of a document containing the hospital discharge letters with related drug therapies of other patients belonging to the aforementioned ward.

According to what is indicated in the aforementioned communication, the aforementioned erroneous entry occurred in 182 ESFs, of which only 49 are active. Given what has been indicated by the Company, only 14 subjects, of the 49 with active FSE, have actually viewed the document erroneously inserted in their FSE. Again according to what was declared on the occasion of the aforementioned notification, only two general practitioners received notifications relating to the inclusion of a new document in the EHR of their patients.

In the aforementioned notification it also emerges that this event would have been generated by a manual error of a technician belonging to the "LOG80 company" and that, after about 6 hours from the aforementioned patient reports, the erroneously entered documents would have been canceled (notification of 4 September 2018, prot. n. 107095). Subsequently, the Company integrated the documentation relating to the aforementioned notification of violation (note 09/10/2018, prot. n. 121623).

2. The preliminary investigation.

In relation to what was communicated by the Company, the Office requested information with a note dated 29.1.2019, prot. no. 3065, to which the Company provided a response with a note dated 03/04/2019, prot. no. 28152, stating, in particular, that:

- «the confirmed users who had accessed their ESF in the short period of time in which the erroneous documentation was present there are 14»;
- «already 6 hours and 30 minutes after taking charge of the report, the documents were eliminated from the ESF in which they had been erroneously deposited»;
- "the LOG80 company, as a precaution, declares that the health documentation sent erroneously could, at most, refer to 182 subjects" and that "only 2 of the 14 citizens who could potentially have had access to the erroneous documentation through the FSE have, with certainty , having accessed health records that are not their own and coincide with the two clients who reported the anomaly»;
- "the LOG80 company is identified as responsible for the treatment" by the Company;
- "the communication to the interested parties has not yet been prepared as, pursuant to art. 34 GDPR, the risk to citizens' rights and freedoms resulting from the violation was assessed as not high, both in consideration of the ascertained data

subjects (...), and in consideration of the time span employed (...) to adopt the immediate measure designed to contain the infringement".

The Office, with deed n. 32245 of 03/13/2019, notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in article 58, paragraph 2, of the Regulation, inviting the aforesaid holder to produce defense writings or documents to the Guarantor or to ask to be heard by the Authority (art. 166, paragraphs 6 and 7, of the Code; as well as art. 18, paragraph 1, of law n. 689 of 11/24/1981).

In particular, the Office, in the aforesaid deed, represented that, on the basis of the elements acquired and the facts that emerged following the preliminary investigation, the Company carried out, by inserting 182 letters of hospital discharge in 14 ESFs of third parties, a communication of data relating to the health of these interested parties to third parties in the absence of a suitable legal prerequisite and, therefore, in violation of the basic principles of treatment pursuant to articles 5 and 9 of the Regulation (art. 5, paragraph 1, letter f) of the Regulation).

With a note dated 11.4.2019 (prot. n. 46587), the Company sent its defense briefs, in which further elements were represented and in particular that:

- "From an immediate analysis of the incident, it was found that the error was due to a massive re-sending of the letters following recovery activities activated manually by a Log80 company technician in the afternoon of 28 August 2018". “As soon as they became aware of the problem, the technical representatives of the Company Information System Operating Unit alerted the Log80 company technicians by telephone, asking them to implement all the necessary measures to correct it and promptly block the incorrect submission. In the meantime, the notification to the Log80 Company was formalized by email, which, around 10.30 on 29 August 2018, blocked the sending of documents in the SOLE/FSE flow and, on the instructions of the Company Information System UO, coordinated with the technicians of Cup 2000 to understand how to amend the situation also as regards relations with general practitioners. At 12.31 the UOC Oncology announced that another patient had received another patient's letter on his FSE. The Log80 company activated the sending of cancellation messages for incorrect pdfs (sent between the afternoon of 28 August 2018 and 10.30 on 29 August 2018): at the same time, Cup 2000 was involved to manage the SUN part. At 4.34 pm on 29 August 2018, the Log80 Company confirmed to the Company Information System Unit that: the technical problem that had generated the error had been resolved; all the pdfs had been deleted from the SOLE network; Cup 2000 had notified the General Practitioners involved of the cancellation; continued to carry out tests and checks

before reactivating the flow of resignation letters to SOLE. At 16.53 on 29 August 2018, the Head of the Company Information System Unit informed the Health Department, the Oncology Unit Management and the SOLE contact person that the system was back up and running, except for sending the documents to SOLE";

- "There can be a maximum of 182 potential patients (and related data) involved in the breach. Of these potential 182, 49 have active FSE and of these 49 patients, only 14 accessed their FSE between the afternoon of 28 August 2018 and morning of 29 August 2018. Finally, there are 2 General Practitioners who have downloaded the discharge letters relating to the patients concerned";

- the Log80 company on the incident declared that: "Due to the report relating to the failure to send the letters to SOLE, we intervened to correct the problem. In this context, a bug has been introduced into the procedure which is illustrated below: the procedure usually automatically sends all the documents produced the previous day at night. In this case a manual launch was carried out at the indicated time following the above signal. The procedure concatenates the pdf of the discharge letter with the pdf of the therapy being discharged. Unfortunately it could happen that, in processing the next patient, the document of the previous patient was not "reset", producing a single pdf document with the concatenation of the documents referring to several subsequent patients. The procedure was immediately stopped on the morning of 29 August 2018 following the first report received. For each mailing made during the period, a cancellation message was sent to Cup 2000 as a precaution which resulted in the cancellation from the FSE. In the afternoon of August 29, all the documents were canceled".

- "The Local Health Authority of Bologna on 21/07/2017 with note prot. no. 88591 appointed the Log80 company as external manager of the processing of personal data, pursuant to the previous Privacy Code, in relation to the contract for the acquisition of maintenance and assistance services for the management system in question". “Subsequently, following the entry into force of EU Regulation 2016/679 and the amendments made to Legislative Decree n. 196/2003 by Legislative Decree n. 101/2018 the same Log80 company was designated - with a note dated 02/13/2019, prot. no. 19222 – responsible for the processing of personal data pursuant to art. 28 of the Regulation”;

- "Following what happened, the Corporate Information System unit, with a view to implementing adequate corrective actions, set a meeting with the Log80 Company for 23 October 2018 so that the Company could adopt the appropriate organizational measures aimed at minimizing the risk of verification of similar events”;

- "Subsequently, with a note dated 15 February 2019, the IT and Communication Technologies UO also asked the Log80

Company to provide evidence of which training/organisational actions had been taken in the meantime. In particular, the Company requested the implementation of explicit tests in a dedicated environment in order to verify the document content and the entire messaging process to be carried out before each restart phase which occurs following any system blocking events". "The Log80 company confirmed the request with a note dated 02/28/2019, prot. no. 26/2019, producing a copy of the internal training report dated 09/25/2018 relating to information security management (Annex in file); copy of corrective action n. 12/2018 produced by Log80's internal management system (Annex in documents).

In relation to the Company's request, dated 16 January 2020, at the Guarantor's Office, pursuant to articles 166, paragraphs 6 and 7, of the Code 18, paragraph 1, by law no. 689 of 11/24/1981 the hearing was held, during which the Company reiterated what has already been represented, specifying in particular that "following a report relating to the circumstance that the flow of data from the management application in the oncology field supplied by the Log 80 company and intended for the FSE, the Company involved the aforementioned supplier to reactivate the flow of documents to the regional FSE. The aforementioned company, having restored the correct functioning of the computer system, in order to ensure that the files were also fed with the clinical documents produced during the period of malfunction of the management application, verified which documents were not transferred to the FSE and proceeded to identify a method for sending them to the regional infrastructure. In order to make this transfer, the aforementioned company has regenerated the pdf. of unsent documents, with the aim of sending them to the regional infrastructure. In this phase, due to a clerical error by the employee of the aforementioned company, instead of the creation of a single document in pdf. for each missing clinical document, a pdf file was generated. that queued multiple documents. It should be noted that the employee of the Log 80 company verified at the end of the file generation operation that the number of documents generated was consistent with the number of documents that had to be transferred to the FSE. In a short space of time, two interested parties, on whose ESF the aforesaid documents had been uploaded, reported this circumstance to the hospital medical staff, who proceeded to inform the company ICT Service, which intervened promptly in order to ensure the cancellation of the documents incorrectly entered in the (49 forty-nine) ESF. Subsequent checks showed that in only 14 (fourteen) cases out of the 49 (forty-nine) cases with an active ESF, the holder of the ESF had access to it in the short period in which the aforementioned documents were present and that only 2 (two) GPs had received in their files the notification relating to the presence of new documents in the ESFs of their clients. Given the extremely rapid intervention with which the documents were canceled (about 6 (six) hours) it was not possible to verify whether in this short period of time the

fourteen aforementioned holders actually had access to the erroneous documentation or, rather, accessed their ESF for other reasons. Of these 14 (fourteen) cases that could have potentially accessed the aforementioned documentation erroneously entered in their EHR, only in two cases (corresponding to the subjects who made the reports) is there certainty of having accessed the aforementioned documentation".

During the hearing, the Company also represented that it had reported to the Emilia Romagna Region "the need to carry out checks - on the regional infrastructure side of the FSE - regarding the size of the documents by type that are uploaded to the Files, compared to the average size of the documents normally sent".

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. the Regulation, in establishing a general ban on the processing of particular categories of personal data, provides for a derogation in the event that the processing is necessary for the purposes of diagnosis, assistance and health therapy (Article 9, paragraph 2, lett. h) and par. 3 of the Regulation) and is carried out on the basis of the law of the Union or of the Member States (see in this regard art. 12, legislative decree n. 179/2012, Prime Ministerial Decree n. 178/2015). The processing of personal data in question can be traced back to the cases indicated in the art. 9, par. 2, lit. h) of the Regulation;

2. due to an error, 182 third party hospital discharge letters were entered in 49 ESFs, including the files of the two interested parties who reported the incident.

4. Conclusions.

In the light of the assessments referred to above, taking into account the statements made by the data controller and data processors during the preliminary investigation and considering that, unless the fact constitutes a more serious crime, whoever, in a proceeding before the Guarantor, declares or falsely certifies news or circumstances or produces false deeds or documents and is liable pursuant to art. 168 of the Code "False declarations to the Guarantor and interruption of the execution of the duties or the exercise of the powers of the Guarantor" the elements provided by the data controller in the defense briefs do not allow to overcome the findings notified by the Office with the deed of initiation of the proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the Local Health Authority of Bologna in

the terms set out in the justification, for violation of articles 5, par. 2, lit. f), and 9 of the Regulation.

In this context, considering, in any case, that the conduct has exhausted its effects, given that the Company has declared that the procedure that led to the erroneous entry of documents in the 14 ESFs has been corrected, that the functioning of the IT system, in order to ensure that the files were also fed with the clinical documents produced during the period of malfunction of the management application and that, having verified the documents not transferred to the FSE, a method was identified for sending of the same to the regional infrastructure the conditions for the adoption of the corrective measures pursuant to art. 58, par. 2, of the Regulation.

5. Adoption of the injunction order for the application of the pecuniary administrative sanction and accessory sanctions (articles 58, paragraph 2, letter i and 83 of the Regulation; article 166, paragraph 7, of the Code).

The violation of the articles 5, par. 2, lit. f), of the Regulations, caused by the conduct put in place by the Local Health Authority of Bologna, is subject to the application of the administrative fine pursuant to art. 83, par.5, lett. a) of the Regulation.

Consider that the Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, has the power to "impose a pecuniary administrative sanction pursuant to article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, according to the circumstances of each single case" and, in this context, "the Board [of the Guarantor] adopts the injunction order, with which it also orders the application of the ancillary administrative sanction of its publication, in whole or in part, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code" (art. 16, paragraph 1, of the Guarantor's Regulation no. 1/2019).

The aforementioned pecuniary administrative sanction imposed, depending on the circumstances of each individual case, must be determined in the amount taking into account the principles of effectiveness, proportionality and dissuasiveness, indicated in art. 83, par. 1, of the Regulation, in the light of the elements provided for in art. 85, par. 2 of the Regulation in relation to which it is noted that:

- the Authority became aware of the event following the personal data breach notification made by the same controller and no complaints or reports were received to the Guarantor on the incident (Article 83, paragraph 2, letter a) and h) of the Regulation);

- the data processing carried out by the Company, through the FSE, concerns data suitable for detecting information on the health of many interested parties. The event led to the inclusion in 182 ESFs (of which only 49 active) of hospital discharge

letters from numerous subjects, even if in only 14 (fourteen) cases, of the 49 (forty-nine) cases with active ESF, the holder of the ESF had access to it in the short period in which the aforesaid documents were present and that only 2 (two) GPs who had received notification in their files relating to the presence of new documents in the ESFs of their clients had access to them (art. 4, paragraph 1, no. 15 of the Regulation and article 83, paragraph 2, letters a) and g) of the Regulation);

- the absence of voluntary elements on the part of the Company in causing the event (Article 83, paragraph 2, letter b) of the Regulation);

- the limited temporal extension of the event and the immediate taking charge of the problem both by the Company's data processor and by the company IT technicians, followed by the identification of corrective and resolution solutions (art. 5 , paragraph 2 and article 83, paragraph 2, letters c) and d) of the Regulation);

- the Company immediately demonstrated a high degree of cooperation, also taking steps to inform the Emilia Romagna Region of the need to carry out checks - on the regional infrastructure side of the ESF - regarding the size of the documents by type that are uploaded to the Files, with respect the average size of the documents normally sent (Article 83, paragraph 2, letters c), d) and f) of the Regulation);

- the Company has already been the recipient of a warning provision pursuant to art. 57, par. 1, lit. a) of the Regulation, for the violation of the basic principles of treatment, pursuant to articles 5, par. 2, lit. f) and 9 of the Regulation (provision of 1 October 2020, n.176);

Based on the aforementioned elements, evaluated as a whole, also taking into account the phase of first application of the sanctioning provisions pursuant to art. 22, paragraph 13, of Legislative Decree lgs. 10/08/2018, no. 101, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 4, lit. a) and par. 5, letter. b) of the Regulation, to the extent of 18,000 (eighteen thousand) euros for the violation of articles 5, par. 1, lit. f) and 9 of the Regulation as a pecuniary administrative sanction deemed, 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 potential number of interested parties and 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 Local Health Authority of Bologna, for the violation of the art. 5, par. 1, lit. f) and 9 of the Regulation in the terms referred to in the justification.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the Local Health Authority of Bologna with registered office in Bologna, via Castiglione, 29 – Tax Code/VAT No. 02406911202, in the person of its pro-tempore legal representative, to pay the sum of 18,000 (eighteen thousand) euros by way of pecuniary administrative sanction for the violations indicated in this provision, according to the methods indicated in the attachment, within 30 days of the notification in the motivation; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the fine imposed.

ENJOYS

to the aforementioned Company, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of 18,000 (eighteen 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, 14 January 2021

PRESIDENT

Station

THE SPEAKER

Station

THE SECRETARY GENERAL

Matthew