[doc. web n. 9739586]

Injunction order against the Parma Local Health Authority - 2 December 2021

Record of measures

n. 420 of 2 December 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 national law 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 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");

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 on the organization and operation of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web n. 1098801;

Rapporteur the lawyer Guido Scorza;

WHEREAS

1. Reporting and notification of infringements

With a note dated XX, Ms XX reported to this Authority an alleged violation of the rules on the protection of personal data for

having received, from the Parma Local Health Authority - located in Parma, Strada del Quartiere n. 2 / A, c.a.p. 43125 - Tax Code 01874230343 - n. 2 reports relating to diagnostic tests concerning two other patients.

In particular, the whistleblower represented that she had received, by registered letter, dated XX, "an envelope containing the outcome of clinical tests carried out at the hospital". The reporting party specified that "The envelope (...) (contained) examinations of other subjects (...) while the report of (...) pertinence (of the reporting party itself) is (must) be totally absent".

With a note dated XX (prot. No. XX), the Healthcare Company sent this Authority a preliminary data breach notification with which it communicated - in relation to this matter - the violation of personal data pursuant to art. 33 of the Regulation, declaring to have sent, on XX date, "(...) reports - by registered letter with return receipt - to a recipient who does not correspond to the name indicated in the reports".

The health authority specified that "in the phase of enveloping the reports, the operator responsible for preparing the envelopes (the internal procedure provides for transmission by registered letter with return receipt) has mistakenly inserted the reports inside the non-matching envelope" , that the violation relates to "personal data (name, surname, date of birth, tax code), contact details (residential address), health data (reports)" referring to no. 2 interested parties and that the data controller became aware of the violation on 24 May, at 12.47.

With the same communication, the Healthcare Company also highlighted that in this case "no IT systems and infrastructures are involved" and that "considering the type of violation, which from an initial investigation is caused by mere human error, being able to provide for substantial changes to the procedures in use, (...) will promote appropriate meetings with all the personnel concerned, in order to test the level of applicability of the procedures on the basis of the number of people assigned to the service and the volume of communications to be made. These meetings will also be useful to collect any improvement proposals from the representatives of the services in the area. (…) The company will make every effort to ensure that periodic random checks are carried out to verify the correct association between the recipient of the package and the holder of the report ".

The Healthcare Company, on XX, sent the Authority a supplementary note (prot. No. XX) of the aforementioned notification of violation, representing having communicated on XX, pursuant to art. 34 of the Regulations, the violation occurred to the two interested parties.

2. The preliminary activity

With a note dated XX (prot. No. XX), the undersigned Office requested the aforementioned health facility, the data controller, for information pursuant to art. 157 of the Code, to be transmitted within 30 days of receipt of the request, in order to have further information concerning the matter, useful for the investigation and evaluation of the case.

With a note dated XX (prot. No. XX), the Company sent its reply to this request for information, highlighting, among other things, that:

- "The security incident that is the subject of the complaint was reported to the writer by e-mail on May 20, u.s. at the address dpo@ausl.pr.it. Due to technical / organizational problems, the email was read by the DPO only on 24 May ";
- "The procedures in use in the 4 business districts provide that, in the event of a positive report, the sending is done by registered letter with return receipt attached to the letter invitation to continue the diagnostic paths. Due to a staff error, two patient reports were placed in the envelope addressed to Ms XX, while Ms XX's was not enveloped. There is therefore no legal basis, but unfortunately it was a mere human error. Ms XX's report was sent by registered letter with return receipt on XX and appears to have been delivered on XX (see attachment 1 - copy of registered return receipt sent to Ms XX) ";
- "the entire outpatient screening procedure" takes place on the basis of an operating manual accessible to staff, to which "(...) the company has provided (...) the operating instructions that can be consulted in the Privacy section of the company intranet (Annex 3 - Operating Instructions) ";
- "the system is entirely managed by organizational divisions of the writer, System management without any intervention by third parties".

Taking into account that the violation described with the notification made by the Healthcare Company pursuant to art. 33 of the Regulation concerns the same object of the proceeding initiated following the report, made on XX, against the same data controller, the two investigative proceedings were brought together and dealt with at the same time pursuant to art. 10, paragraph 4, of the “Regulation no. 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 "[Doc. web 9107633].

On the basis of what is represented by the data controller in the act of notification of violation and of the elements acquired during the investigation activity, as well as the subsequent evaluations, the Office, with deed of XX (prot. No. XX), has notified to the USL of Parma, 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 Regulation.

In particular, the Office, in the aforementioned deed, found that the USL of Parma, by sending a patient an envelope containing no. 2 reports relating to two other patients of the same Company, has carried out, as data controller, a communication of personal and health-related data in the absence of a suitable legal basis and, therefore, in violation of Articles 6 and 9 of the Regulations, as well as art. 2-ter of the Code and the basic principles referred to in art. 5, lett. f), of the same Regulation. In relation to this, the Office has also invited the data controller 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 art. 18, paragraph 1, by law no. 689 of 11/24/1981).

With a note of the twentieth (prot. No. XX), the health authority presented a defense brief, in which, among other things, it highlighted that:

- "The violation - which occurred on the twentieth - occurred in the context of the processes relating to the screening of female cancers; in the present case, the reports of two clients were sent, by registered letter with return receipt, to a non-corresponding recipient, due to an error during the packaging of the same. In the company, all the phases concerning the regional program for the prevention of female tumors are detailed in a special operating manual for 1st level computerized procedures intended for midwives in screening clinics ";
- "The event can certainly not be considered systematic but completely isolated: this assertion is better explained if one takes into account an extremely representative numerical data. If we take into account the time interval between 1 May 2017 and 18 May 2021 (ie from the date of adoption of the Manual and related procedures to the date on which the violation occurred), a total of no. 3756 positive reports, with an annual average of 939 recommended. The report relating to the violation in question appears to be the only one for the entire period considered, or within 4 years ";
- "In terms of seriousness, the communication of the data took place only in relation to the reporting person (who, moreover, received her report on XX, without suffering any prejudice from the violation), so it is unlikely that the deprivation of rights or freedoms, discrimination, economic or social damage, damage to reputation for the two concerned. The two interested parties became aware of the violation following a communication sent by the Company by registered letter with return receipt and one of them contacted the Company Privacy Contact for clarification on the reason for the communication. It is hardly necessary to point out that the telephone conversation ended with a serene and reassuring outcome on the part of the person concerned, who indeed wanted to thank the Company for the important services made available in such a delicate area ";

- "Taking into account the circumstances of the case, the operator's conduct did not have the character of intentionality in causing the violation. In fact, it was a matter of negligent conduct as a consequence of a mere inattention in the enveloping operations, characterized by the character of repetitiveness ";

- "The Company, as soon as it became aware of the violation, immediately intervened, drawing the attention of all operators to the correct management and execution of the procedures", also involving the latter for the purpose of analysis and possible revision improvement of these procedures, as well as planning "(...) a specific training session in October 2021";

- "(...) the Company promptly collaborated (with the Authority) and promptly provided all the information requested (see note prot. XX of the XX)";

- "The Authority became aware of the violation from the whistleblower: the complaint was in fact attached to the report made to the Company on XX";

- "The COVID emergency, as is known, has affected more or less heavily in all aspects of daily life, with repercussions that have been and still are manifold on ordinary work activities. (...) (In order to) address an unknown phenomenon of enormous size, it was necessary to channel many resources into specific training activities, in order to correctly inform the staff on the precautions to be taken, from entering the company to managing the user. (...) This choice, certainly necessary and necessary, together with other factors always linked to the onset and persistence of the pandemic, has obviously limited, if not even eliminated, the possibility of dedicating the usual attention to training and professional updating of various company figures, with imaginable negative repercussions especially on newly hired personnel ".

For the reasons set out above, the Healthcare Company asked the Authority, as a violator, "to consider, after a concrete assessment of the circumstances of the case, the elements provided as suitable for configuring a violation such as to entail the replacement of the sanction financial administration pursuant to art. 83, par. 5, lett. a) with the corrective powers referred to in art. 58, par. 2, lett. a), b) and d) (chap. III, lett. a) of the "Guidelines on the application and provision of administrative pecuniary sanctions for the purposes of Regulation (EU) no. 2016/679 ", adopted on 3 October 2017 by the Article 29 Working Group (" WP 253 ".

3. Outcome of the preliminary investigation

Having acknowledged what was represented and documented during the investigation procedure by the Parma Local Health Authority, first with the acts of notification of violation and, subsequently, with the acknowledgment of the request for

information formulated by the Authority, pursuant to art. 157 of the Code, as well as with the defense statement produced following the act notified by the Authority itself, pursuant to art. 166, it is noted that:

1. 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 should be noted that "personal data" means "any information concerning an identified or identifiable natural person (" interested party ")" and "data relating to health" "personal data relating to physical health or mental health of a natural person, including the provision of health care, which reveal information relating to his state of health "(Article 4, paragraph 1, nos. 1 and 15 of the Regulation);

2. in the health field, 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 basis or subject to written authorization from the interested party (Article 9 of the Regulation and Article 84 of the Code in conjunction with art.22, paragraph 11, legislative decree 10th August 2018, n.101);

3. the data controller is, in any case, required to comply with the principles of data protection, including that of "integrity and confidentiality", according to which 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 accidental loss, destruction or damage "(Article 5, paragraph 1, letter f) of the Regulation);

4. the Company confirmed, both in response to the request for information and in the defense briefs, the communication of data relating to the health of n. 2 interested in a third party not authorized to receive them. This is due to a human error in the envelope phase of the reports. The Company stated that, as soon as the recipient of the aforementioned two reports became aware of the incident, it immediately made changes to the procedures and scheduled a specific training event following a discussion with industry operators.

4. Conclusions

In light of the aforementioned assessments, taking into account the statements made by the data controller during the investigation the truthfulness of which one may be called to answer pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor" the act of initiating the procedure, since none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

For these reasons, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by the Parma USL Company is noted for having processed personal identification data of the interested parties to whom the reports subject to the illegal communication referred to in this proceeding refer, as well as data relating to health in violation of art. 9 of the Regulation and the basic principles referred to in art. 5, lett. f), of the same Regulation.

The violation of the aforementioned provisions makes it applicable, pursuant to art. 58, par. 2, lett. i), the administrative sanction provided for by art. 83, par. 5 of the Regulations, as also referred to by art. 166, paragraph 2, of the Code.

In this context, considering, in any case, that the conduct has exhausted its effects and that suitable assurances have been provided by the data controller, who, in this regard, has implemented specific measures to avoid the repetition of the contested conduct, the conditions for the adoption of prescriptive or inhibitory measures pursuant to art. 58, par. 2 of the Regulations.

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 9 of the Regulations caused by the conduct put in place by the Parma USL Company, is subject to the application of a pecuniary administrative sanction pursuant to art. 83, paragraph 5, lett. a) of the Regulation and 166, paragraph 2, of the Code.

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. 83, par. 2, of the Regulation in relation to which it is noted that:

- the communication of the data concerned two interested parties who, notified by the Company, did not make any complaints (complaints or any type of grievance) (Article 83, paragraph 2, letter a) of the Regulations);

- the communication made by the Healthcare Company involved only one recipient and concerned personal and health data of the two aforementioned patients (Article 83, paragraph 2, letters a) and g) of the Regulation);

- it was an isolated case (see note of XX, prot, no. XX: "between 1 May 2017 and 18 May 2021 - that is, from the date of adoption of the Manual and related procedures to the date on which the violation has been verified - a total of 3756 positive reports were sent, with an annual average of 939 recommended. ") And with respect to the matter there is no malicious behavior on the part of the Data Controller since the violation occurred by mistake in the phase of enveloping the reports (Article 83, paragraph 2, letter b) of the Regulations);

- no measures concerning relevant violations have previously been adopted against the Healthcare Company itself (Article 83, paragraph 2, letter e) of the Regulation);

- the Company has always maintained a clear, precise and collaborative behavior with the Authority (Article 83, paragraph 2, letter f) of the Regulations);

- the Company promptly took action in adopting measures to prevent the occurrence from happening again (Article 83, paragraph 2, letter f) of the Regulation);

- the Healthcare Company, having become aware of the violation following the communication by the reporting party, has notified this violation to the Authority pursuant to art. 33 of the Regulations (Article 83, par. 2, letter h) of the Regulations);

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 € 5,000.00 (five thousand) for the violation of Articles 5, par. 1, lett. f) and 9 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, due to the type of personal data subject to unlawful processing, falling within the particular category referred to in art. 9, paragraph 1, of the Regulations, and the particularity of the illegal event, consisting in a violation of personal data.

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 Parma Local Health Authority - located in Parma, Strada del Quartiere n. 2 / A, c.a.p. 43125 - Tax Code 01874230343 for the violation of art. 5, par. 1, lett. f) and 9 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 USL of Parma, to pay the sum of € 5,000.00 (five thousand) as a pecuniary administrative sanction for the violations indicated in this provision; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the sanction imposed.

INJUNCES

to the aforementioned Healthcare Company, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 5,000.00 (five 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, 2 December 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei