[doc. web n. 9688471]

Injunction order against Società e Salute S.p.a. - May 27, 2021

Record of measures

n. 213 of May 27, 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");

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;

Professor Ginevra Cerrina Feroni will be the speaker;

WHEREAS

1. The violation of personal data.

The Company and Salute S.p.a. (also "Centro Medico Santagostino") has notified a violation of personal data, pursuant to art.

33 of the Regulations, in relation to the successful delivery of a report, through a courier equipped with a specific proxy for collection, to a person other than the recipient, due to human error due to homonymy.

In the same communication it was stated that “common personal data have been violated: name and surname; date of birth; fiscal Code; residential address (e) particular personal data: the type of service that the interested party has benefited from (semen examination); the outcome of the examination carried out ", highlighting that the violation" is entirely due to an internal incidental action. The IT systems and infrastructures (of the Company) were not involved in the incident "(note of the XXth).

With a subsequent note of the XX it was also communicated that the delivery by courier was carried out after several unsuccessful attempts to contact the person concerned by telephone and by e-mail and that disciplinary measures were adopted against the operator responsible for the delivery of the report.

2. The preliminary activity.

In relation to what was communicated by the Company, the Office, with deed of the XXth, prot. n. xx, has initiated, pursuant to art. 166, paragraph 5, of the Code, with reference to the specific situations of illegality referred to therein, a procedure for the adoption of the measures referred to in art. 58, par. 2 of the Regulations, towards the same Company, inviting it 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, l. N. 689 of November 24, 1981).

In particular, the Office, in the aforementioned deed, has preliminarily represented that:

- "The regulations on the protection of personal data provide - in the health field - 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 basis or on the indication of interested party itself subject to written authorization from the latter (Article 9 of the Regulations and Article 84 of the Code in conjunction with Article 22, paragraph 11, Legislative Decree 10 August 2018, n. general of 9 November 2005, available at www.gpdt.it, web doc. n.1191411, deemed compatible with the aforementioned Regulation and with the provisions of decree n. Legislative Decree no. 101/2018) ";
- "the data controller is (...) required to comply with the principles of data protection, including that of" integrity and confidentiality ", according to which personal data must be processed in a manner that guarantees 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 "(Article 5, paragraph 1, letter f) of the Regulations".

Having said that, on the basis of the elements in the documents, with the aforementioned act of the XXth, the Office has deemed that the Company, by delivering, by means of a courier with proxy, a report to a person other than the interested party, has made a communication of data, relating to the health of a patient, to another patient in the absence of a suitable legal basis and, therefore, in violation of the basic principles of the treatment referred to in Articles 5 and 9 of the Regulation.

With a note dated the XXth, the Company sent its defense briefs, in which, in particular, it was declared that:

a) "the alleged violation originated in the delivery phase of the report by proxy, due to a material error of the delivery operator, in accidental violation of the internal procedures relating to the physical delivery of the reports and the identification of patients. The operator in question, failing to promptly verify the date of birth and the tax code of the interested party (or other element that can be inferred from the documentation presented and capable of guaranteeing reliable identification of the same), has printed and delivered the report of a patient to the courier homonym, who is therefore the only interested party involved in the violation ";

b) "the temporal duration of the aforementioned violation was limited in time due to a series of concomitant elements: the notification of the unauthorized third party, in possession of documentation not referring to him, who proceeded to report the incident shortly thereafter the delivery of the report in question by the courier; the prompt intervention of the competent company team, which was immediately activated by carrying out the necessary internal investigations, in order to stop the alleged violation as soon as possible and to obtain the report of its competence from the unauthorized third party ";

c) "as soon as the violation report is received, received by Società e Salute S.p.A. on Friday 4/10/2019 at 6:13 pm, the competent company team was activated, carrying out the necessary checks, and, once the situation had been verified, immediately contacted the unauthorized third party (author of the report), at aim of obtaining the return of the document object of the violation that same evening and, at the same time, proceed with the delivery of the correct documentation "which took place, based on the availability of the third party, on the" following Monday (7/10/2019), the day on which two members of the team effectively obtained the return of the incorrect documentation and provided for the delivery of the correct documentation. Company and Health S.p.A. therefore proceeded to notify the Authority the same evening ";

d) "Having ascertained the unavailability of the person concerned by telephone, Company and Health S.p.A. has communicated the incident to the interested party by email. The interested party has never provided any type of feedback, nor to Società e Salute S.p.A., to date, does it appear that he has ever attempted a contact of any kind, even through a channel

other than e-mail ";

e) "the conduct of the operator that led to the alleged violation is totally attributable to a material error, of an exclusively human nature, due to probable distraction of the operator himself; the nature of the alleged violation therefore appears to be negligent (…); the operator has also expressly stressed several times that he has made a mistake, giving evidence of unintentional behavior ";

f) “a plan of interventions on the IT part (gap analysis and register of updates) was carried out (…), and a regulation on the security of personal data was adopted. (...) ";

g) "the training activity was carried out with a particular focus on the human aspect of IT security (security campaigns, implementation of privacy by design processes to help employees in the correct use of IT tools, promotion of awareness for empower all the professionals on their behavior) ";

h) "following the notification of the violation contested by the Authority, Company and Health S.p.A. also proceeded to "review the" Internal procedure for the physical delivery of the medical report and the results of laboratory tests (...), containing the correct procedures for delivering the reports "and, in addition to what has already been stated, to" evaluate the preparation of a training plan with periodic and constant updating which provides for direct training of the Headquarters Managers, who are then required to distribute the knowledge acquired on their direct subordinates (customer care) ".

The Company then reported "as a mitigating factor applicable to the circumstances of the case, potentially affecting the error of the delivery operator, the attitude of the express courier delegated to collect, having such behavior qualified, according to the operator's words author of the error, as "increasingly hostile and aggressive in his ways, which also culminated in the claim, for example, of not respecting the queue", and characterized by "constant and aggressive (verbally) pressures".

On the occasion of the aforementioned briefs, the document containing "Internal Review-Procedure for the physical delivery of the medical report and the results of laboratory tests" was also sent, showing that:

- "The physical delivery of the medical report takes place through the presentation by the person concerned of the following documents:

report withdrawal form (for laboratory tests) received by the patient upon acceptance;

valid identity document (sufficient in case of missing form).

In the case of a person other than the interested party, physical delivery takes place in a closed and sealed envelope only after

presentation of:

written proxy:

valid identity document of the delegate and the delegator.

In the event of a withdrawal made by a delegate, customer care is required to collect the proxy, a photocopy of the identity document of the delegator and that of the delegate and file everything in the appropriate folder ";

- all the personnel involved have been advised of the obligation to check that the data of the interested party or the delegate actually correspond to the interested party or the person appointed by the delegator and verify the presence of all the required documentation and keep it in a special folder;

- additional operating instructions have been provided, concerning the identification of the interested party and the obligation of confidentiality and secrecy on the information of which the staff becomes aware during the operations.

3. Outcome of the preliminary investigation

Given that, unless the fact constitutes a more serious crime, whoever, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces false documents or documents, is liable pursuant to art. 168 of the Code ("False declarations to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor"), following the examination of the documentation acquired as well as the declarations made to the Authority during the procedure, that the Company has made a communication of data relating to health in the absence of a suitable legal basis, in violation of the basic principles of the treatment referred to in Articles 5 and 9 of the Regulations.

4. Conclusions

In light of the aforementioned assessments, taking into account the statements made by the data controller during the investigation, it is noted that the elements provided by the same in the defense briefs, although worthy of consideration, do not allow to overcome the findings notified by the Office with the act of initiation of the procedure and are insufficient to allow the filing of the procedure, since none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

Therefore, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal health data carried out by the Company, in violation of Articles 5 and 9 of the Regulations.

In this context, considering, however, that the conduct has exhausted its effects - also considering that the Company has provided assurances regarding the return of the document to the interested party and the initiatives implemented in order to

raise awareness among staff and avoid the repetition of the erroneous conduct - the conditions for the adoption of further corrective measures by the Authority, pursuant to 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 and 9 of the Regulations, determined by the processing of personal data, the subject of this provision, carried out by the Company, is subject to the application of the pecuniary administrative sanction pursuant to art. 83, par. 5, lett. a) of the Regulations.

Consider 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 data processing carried out by the Company concerns data suitable for detecting information on the health of a single interested party (Article 83, paragraph 2, letters a) and g) of the Regulation);

- the incident was accidental and caused by a human error, determined, moreover, by a case of homonymy, by an operator who worked for the Company (Article 83, paragraph 2, letter b) of the Regulation );

- the Authority became aware of the violation following the notification made by the data controller who informed the interested party of the incident and no complaints or reports were received to the Guarantor on the incident (Article 83, paragraph 2, lett. h) of the Regulations);

- the Company cooperated fully with the Authority during the investigation and this proceeding (Article 83, paragraph 2, letter f) of the Regulations);

- the data controller promptly took action to remedy the incident and provided for a review of the procedures for the physical

delivery of the report and the results of the laboratory tests (Article 83, paragraph 2, letters c) and d) 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. 5, lett. a) of the Regulations, to the extent of € 10,000 for the violation of Articles 5 and 9 of the Regulation 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.

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

the violation of articles 5 and 9 of the Regulations, declares the unlawfulness of the processing of personal data carried out by the Company under the terms set out in the motivation;

ORDER

to Società e Salute S.p.a (also “Centro Medico Santagostino”), with registered office in Milan, via Temperanza 6, VAT number and CF - 05128650966, in the person of the pro-tempore legal representative, pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, to pay the sum of € 10,000.00 (ten thousand) as a pecuniary administrative sanction for the violation referred to 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 € 10,000.00 (ten 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, May 27, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Cerina Feroni

THE SECRETARY GENERAL

Mattei