[doc. web n. 9732967]

Injunction order against Company H San Raffaele Resnati s.r.l. - November 25, 2021

Record of measures

n. 410 of 25 November 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by Professor Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia, the lawyer Guido Scorza, members and the cons. Fabio Mattei;

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.

With a note from the 20th century, H San Raffaele Resnati S.r.l. (hereinafter the Company) has notified a personal data breach

concerning the insertion of two reports, relating respectively to a blood count and an electrocardiogram, without trace, of a patient inside the envelope intended for another patient and delivered to the same.

In the aforementioned communication, it was highlighted that "the content of the report envelopes is checked through specific corporate organizational procedures (...)".

In relation to the technical and organizational measures adopted to remedy the violation and reduce its negative effects for the interested parties, it was stated that "the documentation erroneously delivered was recovered by the authorized personnel of the Data Controller two hours after the report received by the DPO. The Data Protection Officer jointly with the Quality Office and Occupational Medicine have launched an internal investigation aimed at ascertaining and investigating the causes of the incident, which seems to be attributable to a human error / material error on the part of the bagging officer. ".

It was also stated that the technical and organizational measures adopted to prevent similar future violations were the evaluation of the "revision of the procedures relating to" The Occupational Medicine Process "to the" Management of Occupational Medicine reports "in particular relating to: Preparation for shipment in the presence of Suitability Judgment / Opinion; Preparation for the shipment of examinations of multiple workers; Delivery and shipment of reports "and on the" duration of the sessions and workloads of the bagging staff so that, in order to prevent material errors, appropriate shifts are arranged in order to prevent the loss of concentration deriving from the execution of highly repetitive activities ".

2. The preliminary activity.

In relation to what was communicated by the Company, the Office, with deed of the XXth, prot. n. XX, 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 Company, inviting it to produce defensive 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, l. No. 689 of 24 November 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 sector - 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 (Article 9 of the Regulation and art.84 of the Code in conjunction with art.22, paragraph 11, legislative decree 10 August 2018, n.101);

- 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) .

Having said this, on the basis of the elements in the file, with the aforementioned note of the XXth, the Office has deemed that the Company, by inserting two reports of a patient in the package intended for another patient, has made a communication of data relating to health, 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 Regulations.

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

a) "the Data Breach resulted in the unauthorized communication of (i) a report of a blood count and (ii) a report of an electrocardiogram without a trace (the" Reports ") relating to a single patient using the Services (the "interested party"). This unauthorized communication, (..), occurred due to a clerical error, precisely through the insertion of the Reports in a sealed envelope intended for a third patient (the "Reporter"), received by the latter in turn in the context of the Services ";

b) "the report relating to the blood count taken by the interested party contains clinical values in themselves not indicative of the existence of specific pathologies, intended rather to be interpreted in the context of more precise medical examinations; the electrocardiogram report contains only the words "normal", as it does not have a track and / or any other data suitable for revealing the state of health of the interested party. Therefore, the personal data covered by the Data Breach, in addition to being referable only to the Data Subject, are not by themselves capable of providing information indicative of a specific clinical picture ";

c) "with regard to the duration of the notified violation, it is noted that the Data Breach occurred on the occasion of the receipt, by the Reporter, of the sealed envelope delivered to the Reporter himself and erroneously containing the Reports. On the XXth, the Reporting party then proceeded to inform the Company's Data Protection Officer of the event, (..), via email. Also on XX, a few hours after being informed of the Data Breach, the DPO informed the Company and arranged for an authorized by the Company to immediately recover the Reports erroneously delivered to the Reporter. (..) the Data Breach was subsequently notified to this esteemed Authority on XX ";

d) “in light (…) (i) of the limited number of interested parties (one) and of subjects to whom your personal data have been

erroneously disclosed (one); (ii) the type of personal data subject to communication which, received in isolation and from a person who did not have particular medical skills, and scarcely indicative of the data subject's state of health; and (iii) of the paper transmission method which, unlike the digital one, does not allow easy circulation of the information, which is physically recovered by the Company within a few hours of the report, the violation can be considered of minimal gravity, if not entirely negligible. ";

e) "in order to provide the Services correctly, the Company has adopted two specific procedures: (i) the" Occupational Medicine Process "procedure; and (ii) the "Management of Occupational Medicine Reports" procedure (collectively, the "Procedures"). In particular, on the basis of the Procedures, following the acceptance of patients and the provision of health services requested by the Customers, the results of the examinations carried out are collected and sorted in SISMED and / or, if on paper, in the specific "trays" - correspondence by the competent admissions operator at the Occupational Medicine Secretariat. Once sorted, the test results are collected by the medical staff for reporting. Once the reporting has been completed, the competent secretarial operator takes care of collecting the reports again (obtaining a copy from SISMED where necessary) and placing them in the medical records of the patients to whom they refer. For each medical record, the secretarial operator checks: (i) the presence of all the reports relating to the clinical examinations requested by the Clients; (ii) the completeness and correctness of all personal data relating to the patient; (iii) the presence of the doctor's stamp and signature; as well as (iv) the correctness of the date of execution of the clinical examinations. At the end of this operation, the secretarial operator finally takes care of preparing the reports for shipment, placing them inside an envelope bearing the HSRR header, stamped and sealed. The envelopes, ready for shipment, are kept at the HSRR Occupational Medicine Reports Secretariat. Recipient of the reports in original form is the competent doctor of each Client; a copy of the reports is sent to the patient (where agreed with the Clients); finally, a contact person at each customer is the recipient of the report for sending reports. The Procedures are applied in the manner described so far where, subject to agreement with the Customer, different operating methods are not adopted for the delivery of the reports ";

f) "all the operators involved in the performance of the Services (including health personnel and secretarial operators) have received specific authorization for the processing of personal data, in the form of a privacy contact appointment; as subjects authorized to process personal data, these subjects also receive periodic training on the behaviors to be followed to ensure compliance with the Privacy Law of the processing activities carried out as part of their work at HSRR ";

g) "... the Data Breach that has unfortunately occurred is the effect of a single" human error ", of a carelessness on the part of a single person, moreover occurring only once, in a completely unexpected and random way";

h) "No less relevant is the circumstance of the significant amount of reports to be sent, with specific reference to the historical moment in which the Data Breach occurred: the Company (...) following the almost total suspension of the Services during the March period - May 2020 due to the COVID-19 pandemic, it found itself having to recover a large number of periodic visits, company screenings and examinations requested by customers for their employees, with consequent multiplication of the workload for operators dedicated to the Services themselves (including secretarial operators in charge of packing the reports) ";

i) "any assessment of the subjective element of the conduct by this Authority, should in any case take into consideration the absolute good faith of the Company, interpreted according to the canon specified by the jurisprudence of legitimacy according to which" the exemption of good faith, also applicable to the administrative offense, is found as a cause for the exclusion of administrative responsibility - as is the case for criminal responsibility, in the matter of fines - when there are positive elements capable of generating in the author of the violation the conviction of the lawfulness of the his conduct and it appears that the transgressor has done everything possible to comply with the precept of the law, so that no reproach can be made "(Cassation, civil section VI, no. 12629 of May 13, 2019). In light of this canon, and of the set of technical and organizational measures adopted, there were certainly all the positive elements to generate in the Company the conviction of the lawfulness of its conduct, so no reproach should be made to it ";

j) "the Company has already undertaken some actions aimed at evaluating the possible areas for improvement of the procedures described and / or the security systems adopted, including: guaranteeing greater shifts of the secretarial operators involved, in order to lighten the related load work and avoid, as far as possible, the carrying out of repetitive and / or alienating tasks; the revision of the Procedures, with particular reference to the aspects of (i) preparation for the sending of reports relating to examinations sustained by several patients; (ii) preparation for the shipment of envelopes containing reports and judgments of suitability for the job; and (iii) methods of delivery of reports ".

3. Outcome of the preliminary investigation.

In light of the aforementioned assessments, taking into account the statements made by the data controller 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 or produces false deeds or documents, is liable 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 elements provided by the data controller in the aforementioned defensive briefs, although worthy of consideration, do not allow to overcome the findings notified by the Office with the aforementioned act of initiation of the procedure, since none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

In particular, in relation to the arguments put forward by the Company in the defense briefs, it is noted that, with reference to the error made by the authorized person who carried out the processing operations in question, in the light of consolidated jurisprudence (Cass. Civ. section II of March 13, 2006, no. 5426, Civil Cassation, section II, of April 6, 2011, no. 7885), for the purposes of applying art. 3 of the law n. 689/1981 it is necessary that good faith or error be based on a positive element, foreign to the agent and capable of determining in him the conviction of the lawfulness of his behavior (excusable error). This positive element must not be obvious to the agent with the use of ordinary diligence. In the present case, the agent could have diligently ascertained, through a more accurate check of the data, the correctness of the operations carried out when the report was bagged, thus avoiding communicating health data to an unauthorized third party. .

For these reasons, the unlawfulness of the processing of personal data carried out by the Company H San Raffaele Resnati s.r.l. in the terms set out in the motivation, for the violation of articles 5, par. 1, lett. f) and 9 of the Regulations.

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.

4. 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 Company H San Raffaele Resnati s.r.l., is subject to the application of a pecuniary administrative sanction pursuant to art. 83, par. 5, lett. a) (see Article 166, paragraph 2 of the Code).

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 and of the Regulation, in relation to which it is noted that:

- the data processing carried out concerned information suitable for detecting the state of health of a single person concerned, limited to two examinations (Article 83, paragraph 2, letter a) and g) of the Regulation);
- the incident was accidental and caused by human error by an operator who worked for the Company and the violation had an extremely limited duration (Article 83, paragraph 2, letter a) and b) of the Regulation);
- the Authority has become aware of the violation following the notification made by the data controller and no complaints or reports have been received to the Guarantor on the incident (Article 83, paragraph 2, letter h) of the Regulation);
- the Company collaborated with the Authority during the investigation and this proceeding (Article 83, paragraph 2, letter f) 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 € 6,000 (six thousand) for the violation of Articles 5, par. 1, lett. f) and 9, of the Regulation as a pecuniary administrative sanction, pursuant to art. 83, par. 1 and 3 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 Company H San Raffaele Resnati s.r.l., for the violation of articles 5, par. 1, lett. f) and 9 of the Regulations.

ORDER

pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, to the Company H San Raffaele Resnati s.r.l., with registered office in Milan, Via S. Croce 10 / A, C.F. And. VAT number: 02980270157, in the person of the pro-tempore legal representative, to pay the sum of € 6,000.00 (six 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, of an amount equal to half of the sanction imposed 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 l. n. 689/1981.

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 € 6,000.00 (six 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, November 25, 2021

THE VICE-PRESIDENT

Cerrina Feroni

THE RAPPORTEUR

Cerrina Feroni

THE SECRETARY GENERAL

Mattei