[doc. web n. 9762945]

Order injunction against Azienda USL Toscana Centro - 10 March 2022

Record of measures

n. 85 of 10 March 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stazione, 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 legislative decree 10 August 2018, n. 101 on "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, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and repealing Directive 95/46 / EC ";

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");

GIVEN the documentation in the deeds;

HAVING REGARD to the observations made by the Secretary General pursuant to art. 15 of the Guarantor Regulation n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, Doc. web n. 1098801;

Speaker Dr. Agostino Ghiglia;

WHEREAS

1. Violations of personal data

The USL Toscana Centro company based in Florence, Piazza Santa Maria Nuova, post code 50122 - Tax Code: 06593810481 (hereinafter the "Health Company") notified the Authority of two personal data violations, pursuant to art. 33 of the Regulation, dated XX and XX, concerning, respectively:

a) the delivery “due to a mere clerical error, in response to two separate requests for a copy of a medical record”, of a copy of a medical record to a person other than the interested party.

In relation to this incident, the Healthcare Company announced that:

“The two distinct applicants presented an application to acquire a copy of their respective medical records. The territorially competent company clinical archive (Empoli) made the copies and inserted them, as per procedure, in a closed envelope for delivery to the interested parties. Due to the aforementioned and mere clerical error, n. 2 copies of the same medical record of Ms (omissis) and inserted in two separate packages: one destined correctly for the same (with the modality of collection in presence duly carried out on the XX date) and one destined for the other applicant Mr. (omitted). The latter, once the envelope had been opened and realized the error, sent a communication via email to the Company (dated XX). On the following XX, having read the email, the Soc Servizi ai Citta Firenze - Empoli promptly contacted Mr. (omitted) and on the same morning he was given the correct copy of his medical record and withdrawn the one erroneously delivered by Mrs. (omitted) ":

“The violation involved an interested party” and that “There are no IT systems and / or infrastructures involved”;

“The incident occurred due to a mere error of the archive staff who carried out no. 2 copies of the same document ";

"The personal data subject to the violation are those present in a medical record, that is: personal data; contact details; health data. With particular reference to the latter category, it should be noted that the contents of the file referred to an episode of hospitalization in the traumatology department ";

"There is a company procedure, currently being updated, which governs both the production methods of copies and the preparation of packages, in a sealed envelope, for immediate delivery";

"In light of the short time span in which the data remained in the undue availability of the wrong recipient [from the XX] and the guarantees provided by them in relation to the hypothetical further processing, the risk that confidentiality has been

compromised can be estimated in an average level ";

"Following the communication received from Mr. (omissis) the Data Controller has promptly collected the de quo documentation ".

In this regard, it was also reported that, with a subsequent note of the twentieth century, the Healthcare Company communicated the violation of personal data to the interested party, pursuant to art. 34 of the Regulation, providing reassurances regarding the fact that it has been promptly activated, in order to ask the third party for maximum guarantees to avoid further disclosure of the data subject's personal data. In this regard, the third recipient of the erroneous medical record, with a note - attached to the notification of personal data breach - represented to this health company "that he had not made a copy of said communication or had acquired images and / or photographs, of having promptly returned [to the latter] the documentation and not having communicated and / or disseminated such documentation to other parties ".

b) sending - by ordinary mail - to a third party not entitled to receive it, the report of a client and, to the latter, who is also not entitled to receive, the report relating to the first subject "following mere error of the operator in charge ".

With reference to this matter, the Healthcare Company notified that "two patients, following the carrying out of diagnostic tests carried out at the radiology department of a company hospital, required the delivery of the reports by ordinary analogue mail to their respective residences. On the 20th, the person in charge of the garrison arranged for the preparation of the letters and, subsequently, sent them by post. On the XXth date, the two assisted persons reported, respectively by going to the protocol office and contacting the administrative reception office by telephone, of the erroneous receipt of the report. After carrying out the necessary checks, the Head of the structure activated the procedure for the management of the incident and consequent data breach. It appeared, in fact, that following a mere error of the operator in charge, the reports addressed to the two distinct clients were exchanged in the envelopes and sent by exchanging the recipients ".

In addition, the Healthcare Company, highlighting that "the security incident occurred due to an error by the operator in charge who exchanged the two reports in the mailing envelopes", also pointed out that "following the news of the accident, or the exchange of the patients' reports, the company staff on XX promptly removed the negative consequences of the violation by appointing a company driver to arrange, on the same morning of the XXth, for the direct and short manual collection of the documentation erroneously delivered taking care to: sign a specific declaration in which the patients have declared that they have not made copies and / or reproductions of the reports, that they have not delivered them, even for mere viewing, to other

third parties and, finally, that they have not communicated and / or disseminated the information therein; deliver the correct report ".

With the same communication, the Healthcare Company declared that the organizational measures adopted, also to avoid such material errors, concerned the training of personnel, the updating of indications and operating instructions shared on the company intranet, as well as "the establishment of a company working group on data protection composed of one or more representatives of each company department ".

2. The preliminary activity

The Office, with regard to the cases described above, on the basis of what is represented by the data controller in the respective acts of notification of violation, as well as subsequent assessments, notified the USL Toscana Centro, pursuant to art. 166, paragraph 5, of the Code, the initiation of two proceedings for the adoption of the measures referred to in Article 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), respectively:

a) Act no. XX of the XX, with which the Authority communicated that the violation of personal data notified to the Guarantor, pursuant to art. 33 of the Regulation, dated XX, found the existence of elements suitable to configure, by the Healthcare Company, the violation of the principles applicable to the treatment referred to in Articles 5, par. 1 letter a) and f) and of articles 9 and 32 of the Regulation, as the described conduct configures a communication of data relating to health to third parties in the absence of a suitable legal basis;

b) Act no. XX of the XX with which the Guarantor communicated that the health company has made a communication of data relating to health in the absence of a suitable legal basis and, therefore, in violation of art. 9 and the principles applicable to the treatment referred to in art. 5 of the Regulation.

Following the aforementioned notifications of violations pursuant to art. 166, paragraph 5, of the Code, by the Authority, the Healthcare Company has sent its defense briefs. In particular:

a) with reference to the first case described above (see point 1, letter a)), with a note of the XX (prot. no. XX), without making a specific request for a hearing pursuant to art. 166, paragraph 6 of the Code, the Company, in addition to what has already been represented in the notification of the violation of personal data pursuant to art. 33 of the Regulation, stated that:

- “the cause of the violation must be identified in the mere material error of the operator whose behavior led to the knowledge, by an unauthorized person, of the personal data of a separate interested party (omissis). This is (omitted) a culpable behavior without any intention of causing, knowingly, an unfair prejudice to the confidentiality of the data subject's personal data ";

- "Promptly, only about 36 hours after becoming acquainted with the subject, the company personnel took steps to eliminate the consequences of the violation which, although falling within the judgment of the violation in re ipsa for what concerns the prejudice of confidentiality, allows judge as minor for the following reasons:

1. "from the dialogue with the company staff who managed the contact with the subject, it emerged that the latter (to whom a copy of his file was delivered at the same time) needed to obtain a copy of his file for subsequent health interventions;

2. when, on day XX, he opened and inspected the contents of the envelope, he immediately realized the error since the name of the patient concerned is shown on the front page of the file;

3. therefore immediately sent the communication via email to the Company. It is therefore possible to reasonably exclude access to the details of the information contained in the document body of the folder ";

- "Finally and as already anticipated, it should be noted that the erroneous recipient, in returning the medical record, issued a specific and targeted declaration in which he excluded further processing operations such as, in detail: communication, dissemination, copying, etc. . ";

- "Considering the causes of the violation, which did not involve ICT infrastructures or tools, the choice of the Company, in compliance with the principle of accountability, was guided by the strengthening of organizational measures aimed at segregating functions and immediately introducing a so-called "double check" in the procedure for creating copies and delivering medical records. This control, also in order to integrate the tools to supervise the processing, will be documented electronically with limited access and password protected solutions ";

- "the interested party, also contacted by telephone by the Personal Data Protection Officer, in order to be further made aware of all the detected and relevant elements arising from the violation, has not advanced any claim for compensation and / or any request against the Company (... .), however, and as verbally clarified, appreciated the prompt intervention of the company personnel ";

- "from what was found, the mitigation of the negative consequences guaranteed by the declaration regarding the failure to communicate / disseminate personal data unduly acquired by the erroneous recipient made it possible to contain the severity

of the impact to protect the interested party who, moreover, and as clarified verbally appreciated the prompt intervention of the company staff;

- In addition, the Company confirmed "the need for the medical record to be contained in a sealed envelope" also taking into account that the withdrawal of the same can be handled by a delegate and have adopted a specific "Operating instruction", described in detail in all its steps, the purpose of which is precisely to introduce the aforementioned "double check" in order to "minimize the risk of security incidents in the processing of data during the photocopying of health documentation and preparation of the copy to be delivered to the interested party ".

On this basis, the Company asked the Authority to arrange for the filing of the proceedings or to apply the provisions referred to in art. 58, par. 2 lett. b) of the Regulations;

b) in relation to the second case represented above (see point 1, letter b)), with a note of the XXth, the Healthcare Company, in addition to reiterating what has already been represented in the notification of violation made pursuant to art. 33 of the Regulation, highlighted, among other things, that:

- "the cause of the violation must be identified in the mere material error of the operator whose behavior led to the knowledge, by unauthorized parties, of the personal data of a separate interested party. (…) It appeared, in fact, that following a mere error of the operator in charge, the reports addressed to the two distinct clients were exchanged in the envelopes and sent by exchanging the recipients ";

- "the interested parties, with whom a constructive dialogue was initiated by the company staff, did not reveal any further consequences with respect to the violation that occurred, effectively excluding any prejudice to their rights and freedoms";

- "Given the causes of the violation, which did not involve ICT infrastructures or tools, the choice of the Company, in compliance with the principle of accountability, was guided by the strengthening of organizational measures. A specific operating instruction was adopted which introduces a mechanism of the so-called "Double check" in the procedure for forming / printing the copy of the report, enveloping it and checking before sending. This check is considered suitable in order to verify the correspondence of the report with the holder and recipient of the same ";

“The interested parties (…) have been contacted and constantly updated in order to make them further aware of all the detected and relevant elements arising from the violation, they have not made any further requests and / or claims for compensation. In fact, from what has been noted, the mitigation of the negative consequences guaranteed by the declarations

regarding the failure to communicate and / or disseminate personal data unduly acquired by the erroneous recipient, has made it possible to contain the seriousness of the impact to protect the interested parties who have (...) appreciated the prompt intervention of company personnel ".

For the reasons set out above, the Healthcare Company asked the Authority, as a violator, to "arrange for the filing of the proceedings for the violations highlighted in the Notification of violation Prot.XX, in acceptance of the reasons set out above (...) (o) apply the provisions pursuant to art. 58, par. 2 lett. b) of EU Regulation 2016/679 for the same reasons set out above ".

Taking into account that the violations subject to notification pursuant to art. 33 of the Regulations concern the same data controller and similar cases, the Office has ordered the meeting of the two investigative proceedings, pursuant to art. 10, paragraph 4 of the regulation of the Guarantor n. 1/2019, and communicated this circumstance to the data controller with a note of the XX, prot. n. XX.

3. Outcome of the preliminary investigation

Having taken note of what is represented and documented by the Healthcare Company during the two investigative proceedings referred to in point 1, lett. a) and b), first with the acts of notification of violation and, subsequently, with the related 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;

"personal data" means "any information concerning an identified or identifiable natural person (" interested party ")"; "data relating to health" means "personal data relating to the physical or mental health of a natural person, including the provision of health care, which reveal information relating to his state of health" (art. 4, par. 1, points 1 and 15 of the Regulations). The latter data deserve greater protection since the context of their processing could create significant risks for fundamental rights and freedoms (Cons. No. 51 of the Regulation);

with particular reference to the issues raised, the relevant legislation provides that information on the state of health can be communicated only 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 Article 84 of the Code in conjunction with art.22, paragraph 11, legislative decree 10 August 2018, n.101);

personal data must be processed in compliance with the principles of "lawfulness, correctness and transparency", as well as

"integrity and confidentiality" in order to guarantee adequate security, including protection, by means of adequate technical and organizational measures, from unauthorized processing o offenses and accidental loss, destruction or damage (Article 5, paragraph 1 letter a) and f) of the Regulation);

"Taking into account the state of the art and the costs of implementation, as well as the nature, object, context and purpose of the processing, as well as the risk of varying probability and severity for the rights and freedoms of individuals, the the data controller and the data processor put in place adequate technical and organizational measures to ensure a level of security appropriate to the risk, which include, among others, where appropriate (...) the ability to ensure confidentiality on a permanent basis , the integrity, availability and resilience of the processing systems and services "(Article 32, paragraph 1, letter b) of the Regulation).

3. Conclusions.

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" notified by the Office with the aforementioned acts of initiation of the proceedings, however, none of the cases provided for by art. 11 of the regulation of the Guarantor n. 1/2019.

In particular, the arguments put forward by the Company are not suitable for accepting the archiving requests formulated in the defense briefs.

For these reasons, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by the USL Toscana Centro company is ascertained, in the terms set out in the motivation, in violation of art. 5 par. 1, lett. a) and f), 9 and 32 of the Regulation.

In this context, considering, in any case, that the conduct has exhausted its effects - since, in the two cases of violation in question, the Health Authority declared that the health documentation erroneously delivered to third parties was promptly withdrawn and that the erroneous recipients, at the time of the return of these documents, proceeded to release a specific and targeted declaration with which they excluded further processing operations, such as communications, and to have implemented further technical and organizational measures deemed necessary to prevent future similar events and, in any

case, in order to minimize human error - the conditions for the adoption of prescriptive or inhibitory measures pursuant to 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. a) and f), 9, and 32 of the Regulations caused by the conduct put in place by the Company, is subject to the application of a pecuniary administrative sanction pursuant to art. 83, par. 4, lett. a) and 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, for the present case, it is noted that:

the Authority became aware of the event following the notifications of violation of personal data made by the owner and no complaints or reports were received to the Guarantor on the incident and that the interested parties, in both cases, "appreciated the timeliness of intervention of company personnel "(Article 83, paragraph 2, letters a), h) and k) of the Regulations);

the data processing carried out by the Company concerns data suitable for detecting information on the health of three interested parties (Article 4, paragraph 1, No. 15 of the Regulation and Article 83, paragraph 2, letter g) of the Regulation);

from the point of view of the subjective element, no intentional attitude emerges on the part of the data controller as the violations occurred by mistake in the packaging phase of the health documentation (Article 83, paragraph 2, letter b) of the Regulation);

the Company promptly took charge of the problem by introducing corrective solutions aimed at minimizing human error and therefore the replicability of the same events that occurred (Article 83, paragraph 2, letter c of the Regulations);

the owner has demonstrated a high degree of cooperation with the Authority in order to remedy the violations and mitigate their possible negative effects (Article 83, paragraph 2, letter f) of the Regulation);

a warning was previously adopted against the same health company regarding a relevant violation (provision no.174 of 29 April 2021 web doc no. 9676143) (art.83, par. 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. 4, lett. a) and par. 5, lett. a) of the Regulations, to the extent of € 10,000.00 (ten thousand) for the violation of Articles 5, par. 1, lett. a) and f), 9 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 the regulation of the Guarantor n. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Authority.

WHEREAS, THE GUARANTOR

declares the unlawfulness of the processing of personal data carried out by the USL Toscana Centro Company, for the violation of Articles 5, par. 1, lett. a) and f), 9 and 32 of the Regulation 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 Tuscany Center, with registered office Piazza Santa Maria Nuova, 1 - Florence - P.I. and Tax Code: 06593810481, in the person of the pro-tempore legal representative, to pay the sum of € 10,000.00 (ten 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 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

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 lodge a judicial 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, March 10, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Ghiglia

THE SECRETARY GENERAL

Mattei