[doc. web n. 9693760]

Injunction order against the local health authority of Bari - 22 July 2021

Record of measures

n. 278 of 22 July 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");

GIVEN 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 functioning of the office of the Guarantor for the protection of personal data, Doc. web n. 1098801;

Professor Ginevra Cerrina Feroni will be the speaker;

WHEREAS

1. Reporting

Company XX (a company active in the distribution of some medical devices and linen and mattresses in the hospital sector) has reported that it has received a communication from the local health authority of Bari aimed at acquiring a quote-offer from

the same company for the supply of different types of aids. The note with which the aforementioned communication was made contained the personal data (name, surname, municipality) of about 60 patients to whom the health facilities were intended as well as, in some cases, of the prescriber (note of the XX).

2. The preliminary activity.

In relation to what has been reported, the Office, in the request for information, pursuant to art. 157 of the Code (note of the XX, prot. No. XX), noting that the type of medical devices required for each patient could be inferred from the pathology he suffered, highlighted that, in almost all circumstances, the information communicated is traceable to health data. Therefore, he asked the Company to provide elements regarding the legal assumption that would have allowed the aforementioned transmission of data to Company XX, taking into account that the same communication would seem to have been made exclusively to obtain the presentation of economic offers, for the purchase of medical aids.

The Company, in the person of the Director of the Social and Health District no. 5, provided feedback, representing, in particular, that:

- "for mere clerical error of the administrative assistant cat. C due to a typo and the enormous workload, the notice was published with the names and surnames of the patients written in full. In all previous calls, in fact, and in subsequent ones, the operator has taken care to point all the names of the users entered. (...) In addition, the administrative assistant C, who cannot be dedicated exclusively, having another workload, was also burdened at that time by the burden of the COVID regional contributions (former care allowances) that the Puglia Region has asked to disburse by the end of August, the month in which the shortage of personnel is further aggravated ";
- "it was a single episode and that, in any case, the notice does not contain the indications of the tax code and the date of birth or address of residence of the assisted persons (but only the Municipality because the winning company must be able to calculate the delivery places at the patient's home) does not, in fact, make the user identifiable while safeguarding privacy "(note of the XX, prot. no. XX).

In light of what has been declared, the Office, with act no. XX of the XX, notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in Article 58, par. 2 of the Regulation, inviting the holder 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).

In particular, the Office, in the aforementioned deed, represented that, on the basis of the elements acquired and the facts that emerged as a result of the investigation, the Company, by transmitting to the company XX the aforementioned documentation containing personal data and on the health of some patients , has made a communication of data on health in the absence of the legal conditions provided for by art. 9 of the Regulation and, therefore, in violation of the basic principles of the processing referred to in art. 5 and 9 of the Regulations (Article 5, par. 1, letter f) of the Regulations).

With a note of the XX (prot. No. XX), the Company sent its defense briefs, in which, in addition to what was declared, it was represented that:

- “the name and surname and residence of the assisted persons were erroneously reported during the tender procedure for the supply of prosthetic aids. Please keep in mind the absolutely negligent nature of the RUP of the announcement. (...) Due to a serious shortage of personnel, the undersigned district does not have an administrative collaborator cat. D / organizational position to be dedicated to the tenders that the new legislation requires for the supply of prosthetic aids, in the absence of centralized tenders at company or regional level. (...) We therefore ask you to take into consideration that this was an isolated episode and that in any case the notice did not contain any information that would make the user, in fact, identifiable tout court ";

- steps were taken to "transmit to all the staff working at DSS5 the note concerning" Reference to the regulations on privacy and public employee liability "; request the training office and a copy of the corporate DPO manager (...) for the activation of training sessions for all employees of DSS5 on the subject of privacy in the processing of personal data and related responsibilities of the public employee in the event of non-compliance. (...); provide operational directives to the managers of the DSS5 responsible for the protection of privacy ".

With a subsequent note of the XX (prot. No. XX), the Company requested that "the violation in question pursuant to art. 83 par. 2, letter K of the Regulation, be considered in the light of some clarifications (...): This company, although aware of the sole fault, and not of intent, for having entered some personal data in the first instance, proceeded with the publication of a notice with letter-invitation aimed at acquiring an offer quote for the supply of different types of aids, addressed only to economic operators competent by product category, included in the Register of Suppliers of the Puglia Region "; specifying that "since this is not a public tender, there was no risk of disclosure of personal data to third parties". On the same occasion, the Company also declared that:

- "the personal data have been sent over a closed-loop network, or between this DSS and the companies concerned";

- "in essence, it is believed that what happened is more to be considered a formal error than a substantial one and this is because both this Company and the invited companies have as their common denominator the principle of responsibility and confidentiality on the processing of personal data";

- "the sensitive data that has been sent have been visible only by the companies concerned which, in the event of being awarded, necessarily need to know the name, surname, address and telephone number of the people to whom the requested aids can be delivered";

- "no user has filed a formal complaint with this DSS for what happened and (..) they are the only ones entitled to any reactions".

3. Outcome of the preliminary investigation.

Having taken note of what is represented by the Company in the documentation in deeds and in the defense briefs, it is noted that:

1. the Regulation, in establishing a general prohibition on the processing of particular categories of personal data, provides for exceptions expressly provided for in art. 9, par. 2, of the Regulations;

2. the Company has communicated to company XX and to the other companies competent by product category, included in the Register of Suppliers of the Puglia Region, the personal data, in many cases, including on the health, of about 60 patients, despite the fact that there was no of the exceptions provided for by the aforementioned art. 9, par. 2 of the Regulation.

4. Conclusions.

In light of the aforementioned assessments, taking into account the statements made by the Company 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 o produces false deeds or documents and is liable pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the tasks or exercise of the powers of the Guarantor" the elements provided by the data controller in the defense briefs do not allow to overcome the findings notified by the Office with initiation of the procedure, however, as none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019. This, since the circumstance that "the notice did not contain indications that would make the user, in fact, identifiable tout court" is not relevant for the purpose of excluding the information communicated from the category of "personal data", to the

light of the provisions of art. 4, par. 1, point 1 of the Regulation, personal data means “any information concerning an identified or identifiable natural person (“ interested party ”); the natural person is considered identifiable who can be identified, directly or indirectly, with particular reference to an identifier such as the name, an identification number, location data, an online identifier or to one or more characteristic elements of his physical identity, physiological, genetic, psychic, economic, cultural or social ".

In this regard, it should also be noted that, in relation to the procedure described to replace, generally, the names of users with their initials, the Guarantor has specified on several occasions, that "the practice (...) of replacing the name and surname of the interested party with only initials is in itself insufficient to anonymize personal data (...). Furthermore, the risk of identifying the data subject is all the more probable when, among other things, additional contextual information remains alongside the initials of the name and surname, which in any case make the data subject identifiable "(see par. 3 of the Provv. 243 of 15 May 2014, containing "Guidelines on the processing of personal data, also contained in administrative deeds and documents, carried out for the purpose of advertising and transparency on the web by public entities and other obliged entities", web doc. no. 3134436).

As for the fact, then, that "no user has filed a formal complaint to this DSS for what happened and (..) they are the only ones entitled to any reactions", it should be noted that the Guarantor's control over the relevant regulations on the processing of personal data can be started regardless of the presentation of a complaint, on the basis of reports (Article 144 of the Code) or even ex officio (see lastly, on a similar matter, provision of 14 November 2019, web doc. 9269852).

In relation, then, to the fact that "the personal data were sent over a closed-loop network, or between this DSS and the companies concerned", in addition to highlighting that the transmission of the information was addressed not only to the reporting party XX, but also other companies, does not eliminate the fact that the processing operation carried out, while not integrating the requirements of the dissemination, is attributable to "communication", meaning "the disclosure of personal data to one or more specific subjects other than the interested party, the representative of the owner in the territory of the European Union, the manager or his representative in the territory of the European Union, the persons authorized, pursuant to article 2-quaterdecies, to the processing of personal data under the direct authority of the owner or manager, in any form, including by making them available, consulting or interconnecting "(Article 2-ter, paragraph 4, lett. a) of the Code), as such regulated by the aforementioned art. 9 of the Regulations.

For all of the above, the unlawfulness of the processing of personal data carried out by the local health authority of Bari under

the terms set out in the motivation, for 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.

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 local health authority of Bari, is subject to the application of the pecuniary administrative sanction pursuant to art. 83, paragraph 5, lett. a) of the Regulations.

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

- the communication made by the Company had multiple recipients and concerned data suitable for detecting personal information and the health of numerous interested parties (about 60 patients) (Article 83, paragraph 2, letters a) and g) of the Regulation);

- the absence of willful misconduct on the part of the Company in the cause of the event (Article 83, paragraph 2, letter b) of the Regulations);

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

- no further reports or complaints have been received with respect to the conduct that is the subject of this proceeding (Article 83, paragraph 2, letter h) of the Regulations);

- an injunction order was adopted against the Company on 28 June 2018 for failure to adopt the minimum security measures provided for by Articles 33 and ss. of the Code and rules nos. 3, 4, 5 and 6 of the technical specification referred to in Annex B) of the same Code, in the version prior to the changes introduced by Legislative Decree no. 101/2018 (Article 83, paragraph 2, letter e) 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. b) of the Regulations, to the extent of € 35,000 (thirty-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, also in consideration of the potential number of interested parties and 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 local health authority of Bari, 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 local health authority of Bari with registered office in Bari, Lungomare Starita, 6 - C.F. and P.I. 06534340721, in the person of the pro-tempore legal representative, to pay the sum of Euro 35,000 (thirty-five thousand) as a pecuniary administrative sanction for the violations indicated 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 € 35,000 (thirty-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, July 22, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Cerrina Feroni

THE SECRETARY GENERAL

Mattei