[doc. web no. 9872621]

Provision of 23 March 2023

Register of measures

no. 85 of 23 March 2023

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stazione, president, prof.ssa Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, components, and the cons. Fabio Mattei, general secretary;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as well as on the free circulation of such data and repealing Directive 95/46 /CE, "General Data Protection Regulation" (hereinafter "Regulation");

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national legal 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 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");

HAVING REGARD TO Legislative Decree 10 August 2018, n. 101 containing "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";

CONSIDERING the Regulation n. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved with resolution no. 98 of 4/4/2019, published in the Official Gazette no. 106 of 8/5/2019 and in www.gpdp.it, doc. web no. 9107633 (hereinafter "Regulation of the Guarantor n. 1/2019");

HAVING REGARD to the documentation in the deeds;

GIVEN the observations made by the Secretary General pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the Guarantor's office for the protection of personal data, doc. web no. 1098801;

Speaker Prof. Pasquale Station;

WHEREAS

1. The complaint

With a note dated XX, Mrs. XX, through the lawyer XX, has formulated a complaint concerning the transmission, by the local social-health authority n. 1 of Sassari, dated XX (XX) of an email addressed to the aforementioned complainant, but to an email address not belonging to the same. In particular, the aforesaid e-mail contained the provision (protocol note n. XX) with which the Non-Regional Hospitalization Office, Sassari Health District of the aforementioned Company, authorized the non-regional hospitalization of the complainant, suffering from health problems that cannot be treated in the territory of the Region of Sardinia. According to what was declared and documented by the complainant, the aforesaid document, containing "Hospitalization outside the region in the national territory. Concession of benefits pursuant to Regional Law no. 26/91", sent to the e-mail address: XX not attributable to the complainant, contained, in addition to the identification data of the same, also the indication of the hospital at which to carry out medical treatment and a series of other elements, such as, for example, the presence of the chaperone.

The Office, therefore, with a note dated XX, prot. no. XX asked the local social-health authority n. 1 of Sassari (reiterated against ARES Sardegna with note dated XX, prot. n. XX), pursuant to art. 157 of the Code, elements of information useful for the assessment of the case, with particular reference to the legal prerequisite that would have allowed the transmission of the document containing "Hospitalization outside the region in the national territory. Concession of benefits pursuant to Regional Law no. 26/91", including attachments, to an e-mail address belonging to a subject other than the complainant, as well as in compliance with the principle of integrity and confidentiality (Article 5, paragraph 1, letter f) of the Regulation).

The Company, in acknowledging the note from ARES Sardegna (n. XX of XX) which, in the light of the Regional Law of Sardinia n. 24/2020, of the reform of the Regional Health Service and the consequent deeds, indicated the same local social-health company n. 1 of Sassari as the person competent to provide feedback to the Authority's request for information, declared that:

- "from the reconstruction of the reported facts and the related checks carried out, it appears that, in fact, on the XX date at XX (...) an email was sent by the Extra-regional Admissions Office of the Sassari Health District of this Social Health Authority addressed to the mailbox XX concerning extra-regional hospitalization in the national territory. Concession of economic benefits pursuant to Regional Law 26/9. Due to a mere clerical error by the operator, note XX relating to another client (in this

case the reporting person XX) was sent as an attachment to this email instead of note XX relating to the client XX.";

- "the error, moreover, was reported to the Extra-Regional Hospitalization Office by Ms XX's family member with email dated XX (XX) (...) who subsequently made the necessary corrections" (mail dated XX).

2. Assessments of the Department on the treatment carried out and notification of the violation pursuant to art. 166, paragraph 5 of the Code

In relation to the facts described above, the Office, with a note of the XX (prot. n. XX) notified the local social-health authority n. 1 of Sassari, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation, inviting you to produce defense 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, of law n. 689 of the 11/24/1981).

In particular, the Office, in the aforesaid deed, represented that, on the basis of the elements in the files, it had resulted that the Company had carried out data processing on the complainant's health in violation of the basic principles of the processing referred to in articles . 5 and 9 of the Regulation as well as the safety obligations pursuant to art. 32 of the Regulation.

With a note dated XX, the Company sent its defense briefs, in which, in particular, it highlighted that:

- "the violation occurred only once and involved the transmission by e-mail of an attachment containing data of a personal nature, as well as health, referring to an assisted person (authorization to use services outside the region)";

- "the violation, due to the methods and circumstances in which it occurred, has no intentional character as it can be ascribed to a mere involuntary error by the operator, who in the act of sending the email to the address XX erroneously and in good faith wrong the documentation to be attached, sending note XX (referring to the reporting Ms XX) instead of note XX (referring to the assisted person XX)";

- "that there are no similar previous violations";

- "that the violation concerned the category of personal and health data of the reporting party which, as a result of the transmission method as described above, were involuntarily made accessible to another client who proceeded to inform the sending office of the incident (hospitalizations outside the region) which in turn provided for the correct transmission of the documentation to the interested parties";

- "that no measures referred to in Article 58, paragraph 2, have been previously ordered against the data controller in relation

to the same object";

- "in order to prevent and limit the occurrence of such violations in the future, this Company is organizing special training days, for its staff, to study privacy issues in general and Cyber Security in particular".

3. Outcome of the preliminary investigation

Having acknowledged what is represented by the Company in the documentation in the deeds, in the defense briefs and in the hearing, the following is observed:

1. "data relating to health" means personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information relating to his state of health (art. 4, par. 1, no. 15, of the Regulation). Recital no. 35 of the Regulation then specifies that data relating to health "include information on the natural person collected during his registration in order to receive health care services";

2. the regulation on the protection of personal data provides - in the health sector - that information on the state of health can be communicated to third parties on the basis of a suitable legal prerequisite or on the indication of the interested party himself, subject to written authorization from the latter last (art. 9 of the Regulation and art. 84 of the Code in conjunction with art. 22, paragraph 11, Legislative Decree 10 August 2018, n. 101);

3. the data controller is required to respect 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, through appropriate 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). The adequacy of these measures must be assessed by the data controller with respect to the nature of the data, the object, the purposes of the processing and the risk to the fundamental rights and freedoms of the data subjects, taking into account the risks deriving from the destruction , from the loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed (Article 32, paragraphs 1 and 2 of the Regulation);

4. the conduct of the Company has given rise to a communication of data relating to the complainant's health which conflicts with the basic principles of the treatment pursuant to articles 5 and 9 of the Regulation as well as with the safety obligations pursuant to art. 32 of the Regulation.

4. Conclusions

In the light of the assessments referred to above, taking into account the statements made by the data controller during the preliminary investigation and considering that, unless the fact constitutes a more serious crime, anyone who, in a proceeding before the Guarantor, falsely declares or certifies or circumstances or produces false deeds or documents, it is liable pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the duties or exercise of the powers of the Guarantor" it is represented that the elements provided by the Company in the defense briefs do not allow to overcome the findings notified by the Office with the cited act of initiation of the procedure, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the local social and health authority n. 1 of Sassari, in the terms referred to in the justification, in particular, for having processed personal data in violation of the basic principles of treatment referred to in articles 5 and 9 of the Regulation as well as the safety obligations pursuant to art. 32 of the Regulation.

In this context, considering that the conduct has exhausted its effects, the conditions for the adoption of the corrective measures pursuant to art. 58, par. 2, of the Regulation.

5. Adoption of the injunction order for the application of the pecuniary administrative sanction and accessory sanctions (articles 58, paragraph 2, letter i) and 83 of the Regulation; art. 166, paragraph 7, of the Code).

The violation of the articles 5, 9 and 32 of the Regulation is subject to the application of the administrative fine pursuant to art. 83, par. 4 and 5, of the Regulation.

It should be considered that the Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, has the power to "impose a pecuniary administrative sanction pursuant to article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, according to the circumstances of each single case" and, in this context, "the College [of the Guarantor] adopts the injunction order, with which it also orders the application of the ancillary administrative sanction of its publication, in whole or in part, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code" (art. 16, paragraph 1, of the Guarantor's Regulation no. 1/2019).

The aforementioned pecuniary administrative sanction 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 the light of the elements provided for in art. 83, par. 2, of the Regulation in

relation to which it is observed that:

- the processing concerned data suitable for detecting information on the health of only one data subject (Article 83, paragraph 2, letters a) and g) of the Regulation);

- there is no intentional attitude on the part of the owner, since the violation, relating to an isolated episode, occurred by mistake in identifying the documentation to be attached to the email (Article 83, paragraph 2, letter b) of the Regulation);

- the Company has demonstrated, in particular, a high degree of cooperation with the Authority and no measures have previously been taken against it for pertinent violations (Article 83, paragraph 2, letters e) and f) of the Regulation).

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 4 and 5 of the Regulation, to the extent of 4,000.00 (four thousand) euros for the violation of articles 5, 9 and 32 of the Regulation, as a pecuniary administrative sanction withheld, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary sanction of publication on the Guarantor's website of this provision should be applied, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Regulation of the Guarantor n. 1/2019, also in consideration of the type of personal data subject to unlawful processing.

Finally, it should be noted that the conditions pursuant to art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

ALL THIS CONSIDERING THE GUARANTOR

declares the unlawfulness of the processing of personal data carried out by the local health and social authority n. 1 of Sassari, with registered office in Sassari, Via Alceo Catalocchino, 9 07100 - C.F./P. IVA 02884000908, for the violation of the basic principles of the treatment, pursuant to articles 5 and 9 of the Regulation as well as the safety obligations pursuant to art. 32 of the Regulation, in the terms referred to in the justification;

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the aforementioned local health and social care agency n. 1 of Sassari, to pay the sum of 4,000.00 (four thousand) euros as an administrative fine for the violation 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 fine imposed.

ENJOYS

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 4,000.00 (four thousand) euros according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of adopting 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 entire publication of this provision on the website of the Guarantor and believes that the conditions set forth in art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

Pursuant to art. 78 of the Regulation, of the articles 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision it is possible to lodge an 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 appellant resides abroad.

Rome, 23 March 2023

PRESIDENT

station

THE SPEAKER

station

THE SECRETARY GENERAL

Matthew