[doc. web no. 9891029]

Provision of April 13, 2023

Register of measures

no. 126 of 13 April 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");

CONSIDERING the Legislative Decree 10 August 2018, no. 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 application and the preliminary investigation

With a note dated XX, Dr. XX complained about the dissemination, by ATS Sardegna, on the web, at the url: https://..., of his personal information (date of birth, residence, tax code) and related to health. In particular, a note from the Nuoro ASSL Territorial Pharmaceutical Assistance Service addressed to the Director of the Nuoro ASSL concerning: "Request for the purchase of medicinal product XX" was circulated. This document enclosed a certificate, with unlimited temporal validity, with which it was certified that Mr. XX suffers from cystic fibrosis as well as a note from the Regional Reference Center for Cystic Fibrosis, in which the pathology from which the patient is affected and the drugs he needs were certified.

What was declared by the patient was found, on the XX date, by the Department, in the context of a preliminary verification carried out.

Following the request for information from the Office (note of the XX, prot. n. XX), with which elements of information useful for the assessment of the case were requested, with particular reference to the legal prerequisite that would have allowed the aforementioned dissemination of data personal and health matters, the Extraordinary Commissioner of the ATS Regional Health Liquidation Management, with a note of the XX, requested "the granting of an extension in order to reply to the note in question (...) in order to be able to allow the Local Social Health Authority no. . 3 of Nuoro to acquire further and necessary information fulfilments", representing that "by effect of the Regional Law no. 24/2020, reforming the Regional Health Service, the Sardinia ATS ceased to exist with effect from the XX (…); the local Social Health Authorities have taken over the same, as well as the Regional Health Liquidation Management, with legal personality and patrimonial and economic autonomy, competent for the liquidation of all active and passive positions and all pending lawsuits, from the date of incorporation of the Health Protection Authority (ATS)" and that "having (…) with regard to the note dated XX from the Local Social Health Authority no. 3 of Nuoro, which took over territorial jurisdiction from ATS Sardegna (...)" it is believed "that it is necessary to acquire more and further cognitive elements".

Having accepted the aforementioned request, the local social health agency n. 3 of Nuoro (hereinafter the "Company"), which took over the ownership of the tasks and functions territorially pertaining to the Sardinian ATS, took upon itself the burden of providing feedback on the incident as it refers to the territorial jurisdiction of the Company and, with a note of the XX, declared that:

- "following the knowledge of (the) (..) complaint, this Company performed an initial verification of Dr. XX's grievances, effectively verifying the publication of the documentation of the interested party and immediately de-indexing the erroneously disclosed personal data, thus removing them from the contents of the search engine index. As a result of this operation, the detrimental effects that the event could potentially have caused for the interested party were absolutely avoided, making the erroneous publication harmless for the rights and freedoms of the same ";

- the event "occurred as a result of a mere non-malicious human error consisting in the multiple scanning of the documentation attached to the deed being published instead of the single scanning of the same so as to allow publication only of the attachments necessary for the purposes of the deed adopted";

- "the timeliness of the containment and limitation action put in place by this Company has (...) allowed Dr. XX not to suffer in any way moral and/or material damage consequent to the erroneous publication of his personal data so as to allow to the parties to define and sign a settlement agreement (..) in which this Company only reimbursed Dr. XX for the costs of the law firm's intervention (...) consequent to the drafting and forwarding of the complaint since there was no other damage to which the interested party could have the right and this by express attestation of the latter";

- "the above represented, specifically referring to the transaction signed with the interested party in which the total absence of moral and material damage or infringement of the rights and freedoms of the latter is certified, allows this Authority to carry out its own assessment in the full compliance with the principle of proportionality, having regard to the duration of the violation and the unquestionably culpable nature of the event as well as in consideration of the containment and mitigating measures adopted immediately by this Company, the absence of previous further data violations by the Data Controller and, finally, the cooperation put in place by this Company in carrying out this preliminary investigation phase";

- "as a result and as a consequence of the incident, staff awareness was raised regarding the attention to be paid when publishing the data, especially with regard to the principles of minimization and the need for the same. Furthermore, together with the Company's DPO, special training modules on the processing of data for personnel are being prepared".

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, the Office, with a note dated XX (prot. n. XX), notified the Company, 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, considered that the Sardinian Health Protection Agency (ATS), which was replaced by the local social health authority no. 3 of Nuoro in the ownership of the tasks and functions territorially pertaining to the latter as a result of the Regional Law no. 24/2022, has carried out a treatment of health data in violation of the basic principles of the treatment referred to in articles 5, 6 and 9 of the Regulation as well as articles 2-ter and 2-septies, paragraph 8, of the Code.

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

- "the violation consisted in the erroneous scanning of the documents attached to the interested party's request in such a way as to constitute a single PDF document, instead of three separate ones, and in the consequent erroneous publication of all the documents rather than those solely necessary for the purposes of validity and effectiveness of the administrative deed formed by this Company. Given, therefore, the necessary publication of the administrative deed having been acquired, the erroneous conduct was represented by the further publication of the documents attached to the aforementioned deed and whose publication was not necessary for the purposes of the processing in progress. The violation involved a single interested party";
- "the conduct that caused the violation is of an absolutely culpable nature. It is believed that it should be assessed that in the daily administrative life of the offices of any public body, the duties and obligations are very numerous and, for the most part, to be carried out under conditions of urgency or, in any case, with a certain speed. In this context, one cannot fail to notice how the obligations overlap one another and require attention which, despite the will of the employee, can also diminish with respect to the level that could be required by the activity in progress ";
- "by type and characteristics of the event causing the violation and also by the uniqueness of the same (since no other similar or assimilable situations have ever been reported), it can also be affirmed that the personnel of this Company guarantee absolutely top level attention and work completely respectful and adequate with respect to the daily needs of the administration";
- "in the immediacy of the communication by this Authority steps were taken to de-index the erroneously published data, thus removing them from the contents of the search engine index. As a result of this operation, the detrimental effects that the event could potentially have caused for the interested party were absolutely avoided, making the erroneous publication harmless for

the rights and freedoms of the same. Subsequently to the event, a settlement was reached with the interested party to whom the legal costs incurred as a result of the violation were refunded and a special training session was held for almost all of the administrative staff of the newly established Local Social-Health Agency n. 3 of Nuoro in which both the general principles of reg. EU 2016/679 and Legislative Decree no. 196/2003, that the specific provisions relating to cases of data breach";

- "we proceeded with the study of the specific cases that gave rise to the violation as well as with the analysis of the causes of the event and a standardized procedure is being prepared to be followed in cases of actual or presumed violation. (…) the DPO of the Company proceeded to administer the training to the administrative staff";

- the "Company immediately assumed responsibility for the fact, providing an objective and real reconstruction of what happened, making itself available to (it)(..) the Authority and allowing the latter to be able to fulfill its duties and functions in full and optimal manner".

On the 20th date, the hearing requested by the Company was held. In this circumstance it was specified that:

- "the event occurred during a phase of reorganization of administrative services due to the transfer of powers following the regional health reform";

- "it was an urgent request for a life-saving drug for the patient";

- "in compliance with and to fulfill the legislation on transparency, the request of the requesting structure is generally published";

- "in the scanning of the documentation by the operator, the medical documentation relating to the complainant was also inadvertently included";

- "immediately after learning of the event, the data was immediately deleted and de-indexed from the web and the intervention of the lawyer of the interested party who had presented the request was restored, who declared that there was no any violation of your rights";

- "after this event, the Company requested the DPO (....) to organize a training session for all staff (which was completed in October), in which the aforementioned staff was further sensitized regarding the specific precautions to be kept in the health sector from the point of view of data protection".

3. Outcome of the preliminary investigation

Having acknowledged what was represented by the Company in the documentation in the deeds, in the defense briefs and

during the hearing, it is noted that:

1. the Regulation establishes that personal data must be "processed in a lawful, correct and transparent manner in relation to the data subject ("lawfulness, correctness and transparency"), must be "adequate, pertinent and limited to what is necessary with respect to the purposes for which they are processed («data minimization»)" and "processed in such a way as to guarantee adequate security (…) including protection, by means of adequate technical and organizational measures, against unauthorized or unlawful processing or against the loss, destruction or from accidental damage ("integrity and confidentiality")" (Article 5, paragraph 1, letter a), c) and f) of the Regulation);

2. the processing of personal data is lawful only if and to the extent that one of the conditions provided for by art. 6 of the Regulation. Where personal data are processed for the execution of a task of public interest or connected to the exercise of public powers, their diffusion is permitted only if envisaged by a law or regulation or by general administrative acts (art. 2 -ter, paragraphs 1 and 3 of the Code);

3. with specific reference to information on health, the regulations on the protection of personal data expressly prohibit the dissemination of the aforementioned data (article 2-septies, paragraph 8 and article 166, paragraph 2, of the Code); in the health sector, this information can only be communicated to the interested party and can also be communicated to third parties only on the basis of a suitable legal prerequisite or on the indication of the interested party subject to written authorization from the latter (Article 9 of the Regulation and Article 84 of the Code, in conjunction with Article 22, paragraph 11, Legislative Decree No. 101 of 10 August 2018).

4. Conclusions

In the light of the assessments set out 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 offence, anyone who, in a proceeding before the Guarantor, falsely declares or certifies news 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 the exercise of the powers of the Guarantor"), it is noted that the elements provided by the Company in the defense briefs referred to above and during the hearing are not suitable to accept the requests for dismissal, not allowing to overcome the findings notified by the Office with the aforementioned act of initiation of the procedure.

In the state of the deeds and documentation acquired, in fact, in relation to the described dissemination of Mr. XX, none of the

conditions, among those indicated in the articles 6 and 9 of the Regulation, which could have made the processing of personal data lawful, as represented above.

For these reasons, the unlawfulness of the processing of personal data carried out by the Company is noted, in the terms set out in the justification, for the violation of the articles 5, 6 and 9 of the Regulation as well as art. 2-septies, paragraph 8, of the Code.

In this context, considering that the Company has taken steps to immediately de-index the erroneously disclosed personal data, removing them from the contents of the search engine index, the conditions for adopting 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, 6 and 9 of the Regulation as well as art. 2-septies, paragraph 8, of the Code is subject to the application of the administrative fine pursuant to art. 83, par. 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 Authority became aware of the event following a request from the interested party (Article 83, paragraph 2, letter h) of the Regulation);

the data processing carried out by the Company concerns personal data and data on the health of a data subject (Article 83, paragraph 2, letters a) and g) of the Regulation);

the Company immediately de-indexed the personal data erroneously disclosed, removing them from the contents of the search engine index (Article 83, paragraph 2, letter c) of the Regulation);

The Company 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);

no measures have previously been taken against the controller for relevant violations (Article 83, paragraph 2, letter e) 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. 5, letter. a) of the Regulations, to the extent of 13,000.00 (fifteen thousand) euros for the violation of articles articles 5, 6 and 9 of the Regulation as well as art. 2-septies, paragraph 8, of the Code, 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 social health authority n. 3 of Nuoro, for the violation of the articles 5, 6 and 9 of the Regulation as well as art. 2-septies, paragraph 8, of the Code.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the local social health agency n. 3 of Nuoro, with registered office in Nuoro, Via Demurtas n. 1 – 08100, Tax Code/VAT number 01620480911, to pay the sum of 13,000.00 (thirteen 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 13,000.00 (thirteen thousand) euros according to the methods indicated in the attachment, 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 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, 13 April 2023

PRESIDENT

Station

THE SPEAKER

Station

THE SECRETARY GENERAL

Matthew