[doc. web no. 9572244]

Injunction against the Parma Local Health Authority - 11 February 2021

Register of measures

no. 53 of 11 February 2021

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 the Code regarding the protection of personal data, containing provisions for the adaptation of the national legal system to regulation (EU) 2016/679 (legislative decree 30 June 2003, n. 196, as amended by legislative decree 10 August 2018, n. 101, hereinafter "Code");

CONSIDERING the general provision n. 243 of 15/5/2014 containing the «Guidelines on the processing of personal data, also contained in administrative deeds and documents, carried out for the purpose of publicity and transparency on the web by public subjects and other obliged bodies», published in the Official Gazette no. 134 of 12/6/2014 and in www.gpdp.it, doc. web no. 3134436 (hereinafter "Guidelines of the Guarantor on transparency");

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");

Given 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 Dr. Agostino Ghiglia;

WHEREAS

1. The personal data breach

With a note of the XX, the Parma Local Health Authority (hereinafter the "Company"), communicated to this Authority a violation of personal data, pursuant to art. 33 of the Regulation, representing that:

- «the violation took place through the publication, on the corporate website of the entity www.ausl.pr.it, of two administrative provisions (management decisions) which ordered the exemption from work due to incapacity of two employees who were found to be permanently unfit for the service of the institute, together with the annexed investigative documents containing, the latter, the personal data suitable for detecting the state of health of the interested parties";

- "from a thorough investigation, both of a technical and administrative nature, it emerged that the unauthorized disclosure of personal data contained in the attachments was accidental, as it was exclusively attributable to inattention in the use of the specific function (resume proposal) which allows [through the document management system XX] to resume the draft of the provision»;

- «the operator (in charge of the procedure, pursuant to law 241/1990) has prepared the provision to be proposed to the Manager for adoption, correctly attaching the preliminary documents by "flagging" the "not visible" function; having intervened the need to make changes to the text of the provision, the editor has taken the proposal from the appropriate function without however realizing the loss of the previously assigned setting of (limited visibility) restoring, in fact, the default settings";

- «the documentation of the two interested parties involved was published on the website from 16:32 on 27.06.2018 to 11:04 on 28.6.2018 (interested party 1) and from 18:17 on 27.6.2018 to 11:04 on 28.6.2018 (interested party 2)»;

- "from the technical and IT checks, in this limited period of time, the following consultation attempts resulted:

• doc. id (…) (interested party 1): no. 57, of which no. 12 from within the Company and no. 45 from the outside; of these, no. 28 successful and n. 17 failed due to a down in the register (unreachable);

• doc. id (…) (interested party 2): n. 46, of which no. 16 from within the Company and no. 30 from outside; of these, 14 were successful and n. 16 bankrupts due to the down of the register»;

- «most of the accesses from the outside, both for the doc. id (…) which for the doc. id (...), seem likely to be attributable to the interested party 1 (during the telephone conversations, the interested party 1 stated that he had made several consultations with his mobile device to see if it was a temporary technical problem";

- "in order to avoid the repetition of such a violation, it is decided to adopt the following measure:

• communication to all employees using the so-called [XX] document management information system to pay particular attention to the [resume] function, highlighting how recourse to this command does not affect the settings previously given to the attachments in terms of visibility" .

2. The preliminary investigation

In relation to the aforementioned communication of violation of personal data, the Office with deed no. XX, of the XX, with reference to the specific situations of illegality declared therein, notified the Company, pursuant to art. 166, paragraph 5 of the Code, the initiation of the procedure for the adoption of the provisions referred to in article 58, paragraph 2, of the Regulation, inviting the aforesaid holder 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 11/24/1981).

In particular, the Office, in the aforementioned deed, considered that the violation of personal data notified to the Guarantor pursuant to art. 33 of the Regulation, has detected the existence of elements suitable for configuring by the Company the violations referred to in articles 5, par. 1 lit. a) and c), 9, par. 2 of the Regulation and 2-septies, paragraph 8, of the Code, representing that on the basis of the elements acquired and the documentation in the records, it is ascertained that this Company has published on the institutional website, www.ausl.pr.it, two administrative measures (managerial determinations) which ordered the exemption from work due to incapacity of two employees together with the instruction attachments containing personal data suitable for detecting the state of health of the interested parties.

With a note of the XX (prot. n. XX), the Company sent to the Guarantor its defensive writings in relation to the notified violation, essentially reiterating what was already represented in the notification of the personal data violation.

Specifically, the General Manager of the Company, after having briefly summarized the terms of the matter, represented in particular that:

a) «It was through the use of the "XX" application (determinations), of the "XX" document management information system that the data breach materialized: in fact, it was verified that the attached instruction documents were also published to the decisions»;

b) "Application XX has been in use by the Company since the XX and are configured in such a way as to allow users to prepare the text of the measures with the possibility of attaching accompanying instructional documents and to use the "XX" function which stands for "limited visibility" if these documents contain data or information that by law cannot be disclosed. The

procedure then provides that the manager responsible for signing the deed can directly make changes or delegate them to the user [who drafted the document]. In the latter case, the "Resume" function is used by the latter, which allows you to resume the previously prepared text. At this point, the application immediately launches a pop-up containing the following message "The current determination will be canceled and a copy will be created as a proposal. Do you wish to continue?" This function, being exceptional and occasional, has a peculiarity: by confirming with "OK", the automatically generated copy loses the settings originally assigned to the document, in this case to the attachments, thus resetting these settings to the standard ones. This is what happened in the present case: having received the document for revision in return, the person in charge of the procedure, after having made the requested changes, did not proceed to "biffa" the box relating to the "limited visibility" of the attachments again; nevertheless, the manager";

c) «The processing concerned personal data relating to health. It was necessary for the specific purpose referred to in art. 88, par. 1, of the Regulation, on the basis of the provisions of art. 9, par. 2, lit. b) of the same and by art. 2-sexies, paragraph 2, lett. dd) of the Code, or to fulfill obligations in the field of labor law and social security and protection, in particular for the management and termination of the employment relationship in accordance with the provisions of the law and the National Collective Labor Agreement for the Healthcare Section regarding the assessment of the state of incapacity for health reasons. Were involved in violation no. 2 concerned in their capacity as employees';

d) "The event certainly cannot be considered systematic but isolated, taking into account that in the period 02/11/2017 - 27/06/2018 (i.e. from the date of entry into operation of the applications "XX" and "XX" to the date in which the violation occurred) a total of no. 14 provisions, including resolutions and determinations, which saw the attachment of documents with "limited visibility"; of these, no. 2 measures were affected by human error, among other things by the same operator. In the period 28/06/2018 - 05/04/2019 (i.e. from the day following that of the violation to the day of the last detection), however, no. 4 measures of the same type and characteristics, without registering any errors. Therefore, the error involved 2 measures out of 18 total";

e) «Taking into account the circumstances of the case, the conduct of the user and even more of the Company did not have the character of intentionality in causing the violation. In fact, it was a matter of culpable conduct as a result of a mere inattention in omitting the re-selection of the flag in the box relating to limited visibility";

f) «The Company has done everything in its power to reduce the consequences as quickly as possible and mitigate the effects

of the violation in order to prevent it from continuing or extending to a level or phase that would have had far more serious repercussions. In fact, it promptly limited the impact of the violation on the rights and freedoms of the interested parties, deeming it appropriate to adopt the measure of removing the attachments that were erroneously published. The action of the measure was prompt, so much so that the removal took place 9 minutes after the knowledge of the facts by the Corporate Privacy Representative";

g) "The Company deemed it necessary to ask the developer [of the XX system] to display a text message notifying the user, whenever he uses the "Resume" and "Copy" functions, that the settings previously assigned to the document will be lost. This technical security measure will be structural and not occasional and will be operational from the 30th of the current month";

h) «in the immediate aftermath of the security incident, the Company has in any case once again recommended to all users of "XX" to pay attention to the consequences of the "Resume" function. It did so with an automatic pop-up window containing the following text message: "WARNING While editing a document, the "resume" and "copy" functions from Tools do not save the previously assigned settings. In particular, if the initial choice was to limit the visibility of an attachment, it is necessary to re-flag the "XX" box before sending the document for signature";

i) «During the period in which the documents remained in publication, a total of no. 104 accesses to the two determines; of these, no. 28 there were internal accesses to the Company by the subjects involved in the publication of the documents and in the verification and verification of the violation that occurred; no. 27 failed due to the temporary unattainability of the web page that hosts the online register».

On the 20th date, the hearing requested by the Company was also held at the Guarantor, pursuant to art. 166, paragraph 6, of the Code on the occasion of which it was further represented that

- «compared to the multitude of documents having the characteristics of non-publishability of the attachments to the decision, only in this case did the error object of the notification occur. This was also determined due to the fact that the person in charge of the procedure is assigned to the Fidenza office, while the director of the economic area of human resources, signatory of the decision, is based in Parma, this has prevented direct interlocution between the two subjects»;
- «following the incident, the Company introduced a structural change to the procedure for publishing the decisions, which provides for the highlighting, via an automatic information alert (pop up), of an information message which represents to the operator that, following the modification of the content of the decision, the characteristics relating to the non-publishability of

the document would be lost. Through this system, already operational since the end of April, the operator is required to evaluate whether or not to maintain the non-publishability of the document attachments»;

- Lastly, the Company highlighted that "following the incident, it implemented [further] training activities for the personnel involved in the publication of the decisions" and, given the exceptional nature of the event, asked this Authority "to proceed with the archiving of the administrative procedure and, alternatively, with the exercise of the corrective powers of the Guarantor".

4. Outcome of the investigation

The regulations on the protection of personal data provide that public subjects, when they operate as employers, can process the personal data of the interested parties (art. 4, n. 1, of the Regulation), also relating to particular categories of data, if it is necessary "to fulfill a legal obligation to which the data controller is subject" and, as a rule, for the management of the employment relationship (articles 6, paragraph 1, letter c), 9, par. 2, lit. b) and par. 4 and 88 of the Regulation) as well as "for the execution of a task of public interest or connected to the exercise of public powers vested in the data controller" or for "reasons of significant public interest" (articles 6, par. 1, letter e) and par. 2 and 3; 9, par. 2, lit. g) of the Regulation; 2-ter and 2-sexies of the Code).

The national legislation has also introduced more specific provisions to adapt the application of the provisions of the Regulation, determining, with greater precision, specific requirements for the treatment and other measures aimed at guaranteeing lawful and correct treatment (Article 6, par. 2, of the Regulation) and, in this context, has provided that the processing operations, and among these the "dissemination" of personal data, are permitted only when provided for by a law or, in the cases provided for by law, by regulation (art. 2-ter, paragraphs 1 and 3, of the Code).

In this framework, with regard to the particular categories of personal data, including those relating to health (in relation to which there is a general prohibition of processing, with the exception of the cases indicated in Article 9, paragraph 2 of the Regulation and, in any case a regime of greater guarantee compared to other types of data, in particular, as a result of article 9, paragraph 4, as well as article 2-septies of the Code, the processing is permitted, to fulfill specific obligations "in of labor law [...] to the extent that it is authorized by law [...] in the presence of appropriate guarantees" (Article 9, paragraph 2, letter b), of the Regulation).

In any case, the dissemination of data relating to health is prohibited (art. 2-septies, paragraph 8, of the Code, see also art. 9,

paragraphs 1, 2, 4, of the Regulation), i.e. "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" (Article 4, paragraph 1, no. 15; recital no. 35 of the Regulation). In fact, this provision, already contained in the previous regulatory framework (Article 22, paragraph 8 of the Code, prior to the amendments pursuant to Legislative Decree No. 101/2018), finds further foundation in the regulatory framework outlined by the Regulation which allowed member states to maintain or introduce "further conditions, including limitations" precisely with regard to the processing of data relating to health, similarly to genetic and biometric data (see Article 9, paragraph 4 of the Regulation). In adapting the national legal system to the provisions of the Regulation, art. 2-septies of the Code confirmed the general ban on the dissemination of data relating to health (paragraph 8).

Moreover, since 2014, the Guarantor in the Guidelines on the processing of personal data, also contained in administrative deeds and documents, carried out for the purpose of publicity and transparency on the web by public subjects and other obliged bodies (web doc 3134436), has provided all public entities with specific indications on how to reconcile the transparency and publicity obligations of the administrative action with the right to the protection of the personal data of the interested parties, reiterating the ban on the dissemination of data suitable for revealing the state of health.

Even in the presence of a specific regulatory provision that legitimizes the dissemination or communication of personal data, the data controller is required to comply with the principles of "lawfulness, correctness and transparency", "purpose limitation", "minimization" as well as "integrity and confidentiality" of data and "accountability" (Article 5 of the Regulation).

Given the above, with regard to the present case, the Company confirmed, both in the defense briefs and in the subsequent hearing, the disclosure of the personal data on the health of no. 2 employees on its institutional website www.ausl.pr.it, ascertained by the Guarantor with the note prot. no. 8712 of 12/3/2019, as well as the violation of the provisions notified therewith, albeit caused "by negligent conduct as a result of mere inattention in omitting to re-select the flag in the box relating to limited visibility". The Company also underlined that "following the incident, it introduced a technological, structural change to the procedure for publishing the decisions, which provides for the highlighting, via an automatic information alert (pop up), of an information message which represents to the operator that, following the modification of the content of the determination, the characteristics relating to the non-publishability of the document would be lost. Through this system, already operational since the end of April, the operator is required to evaluate whether or not to maintain the non-publishability of the document attachments»; and to have implemented further training activities for the personnel involved in the publication of executive

decisions.

5. Conclusions

In the light of the assessments referred to above, taking into account the statements made by the owner during the investigation the truthfulness of which may be called upon to answer pursuant to art. 168 of the Code the elements provided by the data controller in the defense brief, although worthy of consideration, do not allow to overcome the findings notified by the Office with the deed of initiation of the procedure, since none of the cases envisaged by the art. 11 of the Regulation of the Guarantor n. 1/2019.

The preliminary assessments of the Office are therefore confirmed and the illegality of the processing of personal data carried out by the Company is noted, as the processing of personal data of the Company's employees took place in violation of articles 5, par. 1 lit. a) and c), 9, par. 2 of the Regulation and 2-septies, paragraph 8, of the Code which provides for the specific prohibition of the dissemination of health data (see already art. 22, paragraph 8 of the previous Code).

The violation of the aforementioned provisions makes the administrative sanction envisaged by art. 83, par 5 of the Regulation, pursuant to articles 58, par. 2, lit. i), and 83, par. 5, of the same Regulation as also referred to by art. 166, paragraph 2, of the Code.

For all of the above, regardless of the notification of the violation of personal data made by the data controller in compliance with the obligation pursuant to art. 33 of the Regulation, the unlawfulness of the processing detected in the case in question, although the result of an occasional malfunction of the aforementioned computer system, nonetheless require the sanctioning intervention of this Authority in today's terms in order to safeguard the fundamental rights and freedoms of the interested.

The violation of the aforementioned provisions makes the administrative sanction envisaged by art. 83, par. 5 of the Regulation, pursuant to articles 58, par. 2, lit. i), and 83, par. 5, of the same Regulation as also referred to by art. 166, paragraph 2, of the Code.

In this context, considering, in any case, that the conduct has exhausted its effects and that suitable assurances have been provided by the data controller, who in this regard has implemented specific technical measures to avoid the repetition of the contested conduct, there are no the conditions for the adoption of measures, of a prescriptive or inhibitory type, 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; 83 of the Regulation; article 166, paragraph 7, of the Code)

The Guarantor, pursuant to articles 58, par. 2, lit. i), 83 of the Regulation as well as of the 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 Board [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 due account the elements provided for by art. 83, par. 2, of the Regulation.

In relation to the aforementioned elements, it was considered that:

1) the detected conduct, held in violation of the regulations on the protection of personal data, led to the dissemination of data on health, of n. 2 employees of the Company, subject to specific protection as, by their nature, they are particularly sensitive taking into account that the processing of such data, in certain contexts, can cause significant risks for the fundamental rights and freedoms of natural persons (Cons. No. 51);

2) the Authority became aware of the violation through the notification of the personal data violation carried out by the Company, dated 29 June 2018 and no reports or complaints were received with respect to the conduct object of this proceeding; furthermore, there are no previous relevant violations committed by the data controller, nor have any provisions pursuant to art. 58 of the Regulation;

3) the data controller did not take into due consideration the indications that the Guarantor has provided to all public entities for some time (see for example, Guidelines on the processing of personal data, also contained in deeds and administrative documents, carried out for purposes of publicity and transparency on the web by public subjects and other obliged bodies mentioned above) and in numerous provisions concerning similar cases (see in particular, provision no. 35 of 13 February 2020, doc. web no. 9285411 and provision of 28 May 2020, no. 92, web doc. 9434609);

4) the conduct «did not have the character of intentionality in causing the violation. In fact, it was a matter of culpable conduct as a result of a mere inattention in omitting the re-selection of the flag in the box relating to limited visibility";

5) the data controller, as soon as he became aware of the violation, has:

implemented corrective measures aimed at eliminating the causes that generated the disputed conduct, in particular, taking steps immediately after the incident to recommend "all users of "XX" to pay attention to the consequences of the "Resume" function. Subsequently, introducing "a structural change to the procedure for publishing the decisions, which provides for the highlighting, through an automatic information alert (pop up), of an information message which represents to the operator that, following the modification of the content of the decision , the characteristics relating to the non-publishability of the document would be lost';

stated that this technical implementation has been operational since the end of April 2019;

collaborated with the Authority during the investigation and in this proceeding.

Due to the aforementioned elements, evaluated as a whole, pursuant to art. 83, par. 2 of the Regulation, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 5, letter. a) of the Regulation, also taking into account the phase of first application of the sanctioning provisions pursuant to art. 22, paragraph 13 of Legislative Decree lgs. 10 August 2018, no. 101, in the amount of 10,000.00 (ten thousand) euros for the violation of articles 5, par. 1 lit. a) and c) and 9 of the Regulation and 2-septies, paragraph 8 of the Code, as a pecuniary administrative sanction withheld, pursuant to art. 83, par. 1, of the same Regulation, effective, proportionate and dissuasive.

Taking into account the particular delicacy of the data disclosed, it is also believed that the ancillary sanction of publication on the website of the Guarantor 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.

It is also believed 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

having detected the illegality of the treatment carried out by the Local Health Authority of Parma, in the terms indicated in the justification, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code

ORDER

to the Local Health Authority of Parma, in the person of its pro-tempore legal representative, with registered office in Strada del Quartiere n. 2/A, 43125 Parma, Fiscal Code and VAT number: 01874230343, to pay the sum of 10,000.00 (ten thousand) euros as an administrative fine for the violations referred to in the justification.

In this regard, it should be remembered that the offender retains the right to settle the dispute by paying an amount equal to half of the fine imposed, within 30 days from the date of notification of this provision, pursuant to art. 166, paragraph 8, of the Code (see also art. 10, paragraph 3, of Legislative Decree no. 150 of 09/01/2011);

ENJOYS

to the same Company to pay the sum of Euro 10,000.00 (ten thousand), in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, 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 no. 689/1981;

HAS

the publication of this provision on the Guarantor's website pursuant to art. 166, paragraph 7, of the Code and by art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019 and it is also believed 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.

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, 11 February 2021

PRESIDENT

Station

THE SPEAKER

guille

THE SECRETARY GENERAL

Matthew