[doc. web no. 9543138]

Injunction order against the San Pio hospital in Benevento - 14 January 2021

Register of measures

no. 22 of 14 January 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, 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 “GDPR”);

CONSIDERING the d. lgs. 30 June 2003, no. 196 containing the "Code regarding the protection of personal data (hereinafter the "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 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");

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 office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web no. 1098801;

Speaker Dr. Agostino Ghiglia;

WHEREAS

1. Introduction

This Authority has received a complaint from Messrs. XX and XX regarding the processing of personal data published on the Intranet of the San Pio Hospital in Benevento.

Specifically, the publication on the company portal of "all the applications presented by employees of the sector [...] and the related selections for economic progression [exposing] all the minutes of the commission and all the evaluation forms drawn up on the same applications was contested signed by employees" – with titles of seniority and professional experience as well as the relative score – referring to around 750 subjects who had applied.

2. Applicable legislation.

Pursuant to the legislation on the matter, "personal data" is "any information relating to an identified or identifiable natural person ("interested party")" and "an identifiable natural person is one who can be identified, directly or indirectly, with particular reference to a identifier such as a name, an identification number, location data, an online identifier or one or more characteristic elements of its physical, physiological, genetic, psychic, economic, cultural or social identity" (Article 4, paragraph 1 , n. 1, of the GDPR).

In this context, the processing of personal data carried out by public subjects (such as the hospital) is lawful only if necessary "to fulfill a legal obligation to which the data controller is subject" or "for the execution of a public interest or connected to the exercise of public powers vested in the data controller" (Article 6, paragraph 1, letters c and e, of the GDPR).

It is also foreseen that «Member States may maintain […] more specific provisions to adapt the application of the rules of this regulation with regard to treatment, in accordance with paragraph 1, letters c) and e), by determining more precisely specific requirements for processing and other measures to ensure lawful and fair processing […]" (art. 6, paragraph 2, of the RGPD).

In this context, it should be remembered that the legislation on the protection of personal data provides that public subjects can "communicate" personal data to subjects other than the interested party only if this operation is provided for "by a law or, in the cases provided by law, regulation" (art. 2-ter, paragraphs 1-4, of the Code)), in compliance - in any case - with the principles of data protection, including that of "purpose limitation" and "minimization", according to which personal data must be - respectively - "collected for specific, explicit and legitimate purposes, and subsequently processed in a way that is not incompatible with these purposes", as well as "adequate, relevant and limited to what is necessary with respect to the purposes for which they are processed" (Article 5, paragraph 1, letters b and c, of the GDPR).

Furthermore, the data controller is required to implement, from the design stage, "appropriate technical and organizational measures [...] aimed at effectively implementing data protection principles, such as data minimisation, and integrating the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects", ensuring that only "the personal data necessary for each specific purpose of the processing" are processed by "default" (Article 25, paragraphs 1 and 2, GDPR).

3. Preliminary evaluations of the Office on the processing of personal data carried out.

With the note of the General Directorate prot. no. XX of the XX, the hospital provided a response to the request for information from the Office (prot. note no. XX of the XX), sending the observations contained in the prot. note no. XX of the XX signed by the XX with various documentation attached.

Following the checks carried out on the basis of the elements acquired and the facts that emerged following the preliminary investigation, as well as the subsequent assessments, the Office with note prot. no. XX of the XX ascertained that the San Pio Hospital of Benevento - making available on its corporate Intranet network, to all employees of the Section Area in possession of accounts and passwords, personal data and information contained in the final ranking relating to the attribution of horizontal economic progressions - Sector Area referring to around 750 of its employees and in the related evaluation forms - has carried out processing of personal data that does not comply with the relevant regulations on the protection of personal data contained in the RGPD. Therefore, with the same note the violations carried out were notified to the hospital (pursuant to article 166, paragraph 5, of the Code), communicating the initiation of the procedure for the adoption of the measures referred to in article 58 , par. 2, of the RGPD and inviting the aforementioned entity to send the Guarantor defense writings or documents and, possibly, to ask to be heard by this Authority, within 30 days (Article 166, paragraphs 6 and 7, of the Code; as well as Article 18, paragraph 1, of Law No. 689 of 11/24/1981).

4. Defensive memories and hearing.

With the note prot. no. XX of the XX the San Pio Hospital of Benevento sent the Guarantor its defense writings in relation to the notified violations.

In this regard, it should be remembered 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 is liable pursuant to art. 168 of the Code, entitled «False statements to the Guarantor and interruption of the performance of the duties

or exercise of the powers of the Guarantor».

Specifically, it was highlighted, among other things, that:

- "On the XX date, the Company had signed an agreement with the Trade Union Organizations [...], also referred to in the minutes of the XX union meeting, to conclude the selection started in the XX year relating to the attribution of the upper economic bracket of the XX year so as to start the selection of the upper economic bracket year XX»;
- «In order to be able to comply with the above agreement and conclude the procedure in the shortest possible time: considering the large number of requests for access to documents pursuant to Law no. no. 241/90 and civic access pursuant to d. lgs. 33/2016, received after the publication of the final ranking and in order to avoid judicial appeals, the Company, in balancing the interests involved, on the one hand the respect of the transparency and publicity obligations and on the other the respect of the obligations relating to privacy, considered transparency to be primary by publishing on its intranet site (circuit that can be consulted only and exclusively by the employee) the files of all the suitable candidates in the ranking, showing the assessments made by the Commission appointed ad hoc for a period, among other things, short (20 days). This made it possible to have the Commission of selection reexamine the scores previously reported on many forms, clarifying interpretative doubts of the announcement, and at the same time to avoid judicial appeals that could have led to the suspension of the procedure";
- «The path followed by this Directorate ended in fact, with a positive result and in full compliance with the agreements signed with the trade unions, as with resolution no. XX of the XX the disbursement was decreed to those entitled, with the month of December XX of the upper economic bracket year XX, and with the resolution of the XX the selection was started for the attribution of the upper economic bracket year XX which ended , with the disbursement of the same, with the monthly salary of July 2020";
- "Finally, this Guarantor is brought to the attention that [...] no report and/or appeal has been received by this Company from the legitimate owner of the personal data".

On the 20th date, the hearing requested by the San Pio di Benevento hospital was also held at the Guarantor pursuant to art. 166, paragraph 6, of the Code on the occasion of which it was represented, in addition to what has already been reported in the documentation sent, that:

- «the procedure underlying the successful publication of the data on the company intranet is connected to the fulfillment of

trade union agreements signed with the company management following a meeting with the Prefect (whose minutes are already in the proceedings before the Guarantor). The procedures concluded positively, with the disbursement of the higher economic bracket for company employees for year XX and subsequently also for those who participated for year XX";

- «none of the participants in the selection contacted the administration to contest the legitimacy of the data entry on the Intranet»;

- "the Postal Police, already the recipient of reports on the same case by only two trade union organizations (among other things, signatories of the aforementioned agreement) closed the case";

- «it was not possible at the beginning to establish the precise number of those entitled to the higher band, because it was linked to the size of the funds. Therefore, the number of those who were able to have the higher category in enjoyment was established subsequently, i.e. at the moment in which the calculation could be made on the basis of the number of participants, categories and economic category in enjoyment prior to the XX".

5. Outcome of the investigation relating to the complaint presented

The subject of the specific case brought to the attention of the Guarantor is the successful publication, on the Intranet network of the San Pio di Benevento Hospital, accessible to all employees via username and password, of personal data and information contained in the final ranking relating to the attribution of horizontal economic progressions - Sector Area referring to approximately 750 employees, as well as in the related evaluation forms, which contained, in addition to the identification data, also information relating to length of service, with relative qualifications, and professional experiences (qualifications of study, teaching activity, courses followed) with indication of individual scores.

Both in replying to the Office's request for information and in the defense briefs, the hospital confirmed the online publication of the aforesaid documentation containing the personal data described, representing in any case that the personal data object of the complaint "remained published, on said internal site [i.e. the company Intranet], for a period of approximately 20 days (XX-beginning XX» (cf. note prot. no. XX of XX sent via note from the General Management prot. no. XX of XX).

The publication of data on an intranet with selective access - involving the knowledge «of personal data to one or more specific subjects other than the interested party [...] in any form, including by making them available, consulting or by interconnection» (art. 2-ter, paragraph 4, letter a, of the Code) - involves a "communication" of personal data to third parties, permitted only in cases where it is provided for "by a law or, in cases provided by law , of regulation" (art. 2-ter, paragraphs 1-4, of the Code).

In this regard, in the defensive writings of the hospital, no regulatory assumption was indicated that could legitimize the aforementioned communication of personal data, pursuant to the aforementioned art. 2-ter, paragraphs 1-4, of the Code. To this end, in fact, the state sector legislation on transparency (legislative decree n. 33 of 14/3/2013) does not provide for any form of mandatory publicity of the final ranking relating to the attribution of horizontal economic progressions or employee evaluation forms.

As for the methods for complying with the principles of "purpose limitation", data "minimization" and proportionality, it is necessary to remember that - based on the new privacy by design and by default models introduced by the GDPR - the data controller is required to implement, from the design stage, "appropriate technical and organizational measures [...] aimed at effectively implementing the principles of data protection, such as minimisation, and at integrating the necessary guarantees in the processing in order to meet the requirements of the this regulation and protect the rights of data subjects», ensuring that only «the personal data necessary for each specific purpose of the processing» are processed by «default» (Article 25, paragraphs 1 and 2, GDPR).

In this regard, the hospital stated that the publication on the intranet of all the personal data described above was necessary "To be able to comply with the [trade union] agreement and conclude the procedure in the shortest time possible: considering the large number of requests from 'access to the documents pursuant to l. no. 241/90 and civic access pursuant to d. lgs. 33/2016, received after the publication of the final ranking and in order to avoid judicial appeals [...]". This need was also reaffirmed during the hearing where it was highlighted that "the procedure underlying the publication of data on the company intranet is connected to the fulfillment of trade union agreements signed with the company management following a meeting with the Prefect (the minutes of which are already in the records of the proceedings before the Guarantor)".

Indeed, for the stated purpose, i.e. the response to access requests, the publication on the Intranet of data and information concerning all employees, does not appear to comply with the requirement of data protection by design (Article 25, paragraph 1, of the RGPD), considering - among other things - that, in this way, all the guarantees provided for the counter-interested subjects for the protection of privacy and their personal data are lost, including the possibility of presenting a possible opposition, from the specific disciplines sector (cf. art. 5, paragraph 5, of Legislative Decree no. 33/2013; art. 22, paragraph 1, letter c, of Law no. 241 of 08/07/1990; art. 3, of Presidential Decree no. 184 of 12/4/2006).

For all of the above, the circumstances highlighted in the written defense considered as a whole, certainly worthy of

consideration for the purpose of assessing the conduct, are not sufficient to allow the dismissal of the present proceeding pursuant to art. 11 of the Regulation of the Guarantor n. 1/2019.

In this context, the findings notified by the Office with the note prot. no. XX of the XX and the non-compliance of the processing of personal data object of the complaint with the relevant regulations on the protection of personal data is noted, as the hospital:

- has carried out a "communication" operation of personal data to subjects other than the interested party, in the absence of the provision of a specific "rule of law or, in the cases provided for by law, of regulation", in violation of art. 2-ter, paragraphs 1-4, of the Code and of the art. 6, par. 1, lit. c) and e); par. 2 and par. 3, letter. b) of the GDPR;

- has processed personal data that is not "limited to what is necessary with respect to the purposes for which they are processed" and therefore not respecting the principle of "data minimization", in violation of art. 5, par. 1, lit. c) of the GDPR.

- has not adopted adequate "technical and organizational measures" "to effectively implement data protection principles" from the design stage and to ensure that only "personal data necessary for each specific purpose of the processing" are processed », in violation of the art. 25, par. 1 and 2 of the GDPR.

Considering, however, that the conduct has exhausted its effects, as the data controller has taken steps to remove the personal data object of the complaint described above from the company intranet, without prejudice to what will be said on the application of the pecuniary administrative sanction, we do not the conditions exist for the adoption of further corrective measures pursuant to art. 58, par. 2 of the GDPR.

6. Adoption of the injunction order for the application of the administrative fine (articles 58, paragraph 2, letter i; 83 GDPR)

The San Pio di Benevento hospital appears to have violated articles 5, par. 1, lit. c); 6, par. 1, lit. c) and e), par. 2 and par. 3, letter. b); 25, par. 1 and 2 of the GDPR; as well as the art. 2-ter, paragraphs 1-4 of the Code.

For the violation of the aforementioned provisions - also considering the reference contained in the art. 166, paragraph 2, of the Code – the application of the administrative sanctions pursuant to art. 83, para. 4 and 5 of the GDPR.

In this regard, the art. 83, par. 3, of the GDPR, provides that «If, in relation to the same treatment or related treatments, a data controller or a data processor violates, with malice or negligence, various provisions of this regulation, the total amount of the pecuniary administrative sanction will not exceeds the amount specified for the most serious violation".

With regard to the conduct in question, therefore, the violation of the aforementioned provisions is subject to the more serious

administrative pecuniary sanction provided for by art. 83, par. 5 of the GDPR, which therefore applies to the present case.

The Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the GDPR, as well as art. 166 of the Code, has the corrective 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, depending on the circumstances of every single case". In this framework, «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, according to 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 GDPR.

In this sense, the detected conduct in violation of the regulations on the protection of personal data concerned the mere communication of personal data to specific subjects, authorized to access the company intranet using their own credentials. The personal data processed, referring to around 750 employees, does not belong to particular categories or to criminal convictions or offenses (articles 9 and 10 of the GDPR) and publication on the Intranet lasted for a limited time of around 20 days. The conduct held, based on an incorrect assessment of the relative compliance with the legislation on the protection of personal data, is of a negligent nature. The hospital has collaborated with the Authority during the investigation of this proceeding and there are no previous relevant violations of the GDPR committed by the aforementioned company. It should also be considered, as a further mitigating element, the context in which the treatment took place and the need to fulfil, in a short time, "the trade union agreements signed with the Company Management following a meeting with the Prefect" for the purposes of starting of the internal procedures for the attribution of the economic progression brackets to all the personnel concerned, arrears over the years. In this situation, in fact, the administration - also considering that "it was not possible at the beginning to establish the precise number of those entitled to the upper band, because it was linked to the consistency of the funds" - was faced with a "large number of requests of access to the documents pursuant to l. no. 241/90 and civic access pursuant to d. lgs. 33/2016, received after the publication of the final ranking", for which he deemed it necessary to make the procedure extremely transparent. Furthermore, according to what was declared by the institution, none of the participants in the selection had previously "applied to the administration to contest the legitimacy of the data entry on the intranet".

Based on the aforementioned elements, evaluated as a whole, it is deemed necessary to determine pursuant to art. 83, para. 2

and 3, of the RGPD, the amount of the pecuniary sanction, provided for by art. 83, par. 5, of the RGPD, in the amount of 10,000.00 (ten thousand) euros for the violation of articles 5, par. 1, lit. c); 6, par. 1, lit. c) and e), par. 2 and par. 3, letter. b); 25, par. 1 and 2 of the GDPR; as well as the art. 2-ter, paragraphs 1-4 of the Code, as a pecuniary administrative sanction deemed effective, proportionate and dissuasive pursuant to art. 83, par. 1, of the same GDPR.

In relation to the specific circumstances of the present case, relating to the publication of employee personal data on the company intranet in the absence of an appropriate regulatory basis, it is also believed that the ancillary sanction of publication of this provision on the website of the Guarantor must be applied , provided for by art. 166, paragraph 7, of the Code and by art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019.

Finally, it is believed that the conditions set forth in art. 17 of the Regulation of the Guarantor n. 1/2019.

ALL THIS CONSIDERING THE GUARANTOR

having detected the illegality of the treatment carried out by the San Pio di Benevento Hospital in the terms indicated in the justification pursuant to articles 58, par. 2, lit. i) and 83 of the GDPR

ORDER

to the San Pio di Benevento Hospital, in the person of its pro-tempore legal representative, with registered office in Via Dell'Angelo 1 - 82100 Benevento (BN) - Tax Code 01009760628 to pay the sum of 10,000.00 (ten thousand) euros as an administrative fine for the violations referred to in the justification;

ENJOYS

to the same hospital to pay the sum of 10,000.00 (ten 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 no. 689/1981.

It should be remembered that the offender retains the right to settle the dispute by paying - always according to the methods indicated in the annex - an amount equal to half of the fine imposed, within the term set out in art. 10, paragraph 3, of Legislative Decree lgs. no. 150 of 09/01/2011 envisaged for the lodging of the appeal as indicated below (art. 166, paragraph 8, of the Code).

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;

- annotation in the Authority's internal register pursuant to art. 17 of the Regulation of the Guarantor n. 1/2019.

Pursuant to art. 78 of the GDPR, 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, 14 January 2021

PRESIDENT

station

THE SPEAKER

guille

THE SECRETARY GENERAL

Matthew