SEE ALSO NEWSLETTER OF 30 JUNE 2022

[doc. web n. 9784482]

Injunction order against the Local Health Authority of Rome 1 - 26 May 2022

Record of measures

n. 199 of 26 May 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, Professor Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, members and dr. Claudio Filippi, Deputy Secretary General;

GIVEN the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/4/2016, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95 / 46 / EC, "General Data Protection Regulation" (hereinafter "RGPD");

GIVEN the d. lgs. n. 196 of 30/6/2003, containing the Code regarding the protection of personal data (hereinafter the "Code");

GIVEN 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 advertising and transparency on the web by public entities and other obliged entities", published in the Official Gazette. n. 134 of 12/6/2014 and in www.gpdp.it, doc. web n. 3134436 (hereinafter "Guidelines on transparency");

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

GIVEN the documentation in the deeds;

GIVEN the observations made by the Secretary General pursuant to art. 15 of the Guarantor Regulation n. 1/2000 on the organization and operation of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web n. 1098801;

Rapporteur the lawyer Guido Scorza;

WHEREAS

1. Introduction

This Authority has opened an investigation against the local health authority Rome 1 (ASL Rome 1) in relation to a violation of the legislation on the protection of personal data, resulting from the dissemination of personal data on the related institutional website.

Specifically, as emerged from the preliminary verification carried out by the Office, it was possible to access a web page (https : // ...) where there were two files titled:

1. "XX access register", containing the "provisional register of requests for access to documents" referring to 1119 requests, with specific indication of the following data: register number, date and protocol number, subject, sender, recipient (url: https : // ...).

2. "Register of accesses XX", containing the "provisional register of requests for access to documents" referring to 218 requests, with specific indication of the following data: register number, date and protocol number, subject, sender, recipient (url: https : // ...).

The aforementioned documents contained, in the subject and sender field, personal data and information, with specific indication of the name of the interested party or of its legal representative, or both. In a very significant number of cases, data relating to the health of the subjects concerned were also contained, considering that the type of documents requested from the ASL, in most of the accesses, was inherent to health documentation (including medical records, invalidity assessments, tests , technical reports, etc.). Furthermore, in the subject field, it was possible to frequently find further detailed descriptions of what was requested, with clear indications always to data on the health of the subjects concerned (just to give a few examples, it was indicated according to the individual cases: "visit of the XX at the first instance commission for the assessment of disability states ";" Request for acquisition of toxicological analyzes ";" copy conforming to the original clinical examinations, psychiatric examination and psychodiagnostic tests ";" Request for a copy of the attention function tests on plain paper " ; "[...] delivery of the ultrasound documentation including ultrasounds - radiographs and reports of all the examinations carried out from 2009 to 2010"; etc.).

2. The legislation on the protection of personal data

Pursuant to the relevant regulations, "personal data" is "any information concerning an identified or identifiable natural person (" interested ")" and "the natural person who can be identified, directly or indirectly, with particular reference to a identifier such

as the 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 "(art. 4, par. 1 , No. 1, of the GDPR).

The GDPR also defines "health data" as "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 , para. 1, no. 15; recital no. 35).

In this context, public entities, such as the ASL, can generally disclose "personal data" in accordance with the provisions of art. 2-ter, paragraphs 1 and 3, of the Code, and - in any case - in compliance with the principle of "minimization", according to which personal data must be "adequate, relevant and limited to what is necessary with respect to the purposes for the which are processed "(Article 5, paragraph 1, letter c, of the GDPR).

Data relating to health, on the other hand, fall within the "particular categories of personal data", for which it is envisaged - also for the protection of individuals and in "respect for human dignity, fundamental rights and freedoms of the person" (art. 1 , paragraph 1, of the Code) - an express prohibition of dissemination, that is the possibility of giving them "knowledge [...] to indeterminate subjects, in any form, including by making them available or consulting" (art. 2-septies, paragraph 8; Article 2-ter, paragraph 4, letter b, of the Code; Article 9 of the RGPD, paragraphs 1, 2 and 4). The same prohibition is also recalled by the state regulations on transparency, in the part in which it provides that "The limits [...] on the dissemination of data suitable for revealing the state of health [...] remain valid" (Article 7-bis, paragraph 6, legislative decree n. 33/2013).

With particular reference to the case in question, the opportunity to establish "in each administration a register of access requests submitted (for all types of access)" is indicated in the ANAC Guidelines on civic access, adopted by agreement with the Guarantor (par. 9, Determination no. 1309 of 28/12/2016 containing the "Guidelines containing operational indications for the purpose of defining the exclusions and limits to civic access pursuant to art. 5 co. 2 of Legislative Decree 33/2013 », in Official Gazette no. 7 of 10/1/2017 and in

http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6666.

However, in the same Guidelines it is specified that the register contains "the list of requests with the subject and the date and the relative outcome with the date of the decision" and is published on the website "obscuring any personal data present" (therein . of the same tenor also par. 8.2.b. of the Circular of the Minister for Public Administration no. 1 of 2019, containing "Implementation of the rules on generalized civic access (so-called FOIA)", in http: //www.functionpublic .gov.it / sites / public

function.gov.it / files / Circolare_FOIA_n_1_2019.pdf).

It is also necessary to take into account that the same state regulations on transparency expressly provide that "Public administrations may order the publication on their institutional site of data, information and documents that they are not obliged to publish pursuant to this decree or on the basis of a specific provision of law or regulation, in compliance with the limits indicated in article 5-bis, proceeding with the anonymous indication of any personal data present "(article 7-bis, paragraph 2, of Legislative Decree no. 33/2013).

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

From the checks carried out on the basis of the elements acquired and the facts that emerged as a result of the investigation, as well as subsequent evaluations, the Office with note prot. n. XX of the XX has ascertained that the local health authority Rome 1 - by disseminating the personal data and information contained in the documents published online described above - has carried out a processing of personal data that does not comply with the relevant regulations on the protection of personal data contained in the GDPR. Therefore, with the same note the violations carried out (pursuant to art. 166, paragraph 5, of the Code) were notified to the aforementioned ASL, communicating the start of the procedure for the adoption of the measures referred to in article 58, par. 2, of the RGPD and inviting the administration to send to the Guarantor defensive writings or documents and, if necessary, to ask to be heard by this Authority, within the term of 30 days (Article 166, paragraphs 6 and 7, of the Code; as well as art.18, paragraph 1, of law no. 689 of 11/24/1981).

4. Defensive memories.

The local health authority of Rome 1, with note prot. n. XX of the XX, sent to the Guarantor his defense writings in relation to the violations notified.

In this regard, please note that, unless the fact constitutes a more serious crime, anyone who, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces false documents or documents, is liable pursuant to art. 168 of the Code, entitled "False statements to the Guarantor and interruption of the performance of the tasks or the exercise of the powers of the Guarantor".

In this context, with regard to the conduct held, the Entity has in particular represented, among other things, that:

- "Upon receipt of the communication from this Authority [...], numerous analysis and remediation actions were promptly implemented [indicated in the documents]";

- "from the main analysis carried out at the specific transparent Administration section - Subsection Other contents - it emerged that the files in question were found to have been uploaded to the back end of the company website due to a mere clerical error, due to the loading of the provisional Register file instead of the definitive one, as can be seen from the name of the table that appears when the electronic document is opened ";

- "In fact, as for the other years of the Register, the provisional files constitute" worksheets "aimed only at creating the file of the Annual Access Register, a file that has been specially processed and purged of the identification data present in the provisional file, to guarantee the 'anonymisation of the applicants / subjects involved, are then, as a rule, published in the dedicated section ";

- "The clerical error is also inferred from the fact that for all the other years subject to publication the problem is not clear";

- "Precisely to ensure greater supervision of the documentation publication process, already in 2018, the Company had arranged for the contracting of the supplier [identified in the documents] who provided the Company with the platform [identified in the documents, which ] allowed, for the years to come, the correct feeding and publication of data in the Transparent Administration section […] »;

- "The application solution [used], whose access is limited to accredited users only, offers protection, security and prevention mechanisms from undue intrusions, both at the software level and at the infrastructural level [described in the documents]";

- "The Company has also created specific guidelines, with the support of the company DPO, for the correct publication of the files in compliance with the legislation on the processing of personal data [...]";

- "with regard to the data present in the files in question, no report or complaint from any interested party has ever reached the undersigned Company or, as far as is known, to other Authorities";

- "The IT process [...] presents a level of practicability of particular complexity and of little immediacy, which allows us to state that the possibility of considerable access [to the disputed files] was completely remote".

5. Evaluations of the Guarantor

The issue that is the subject of the case submitted to the attention of the Guarantor concerns the dissemination of personal data and information, contained in the "Access register" received by the ASL, relating to the years XX and XX, published online (referred to in the files identified above at nos. . 1 and 2 of par. 1).

The aforementioned registers clearly reported all the names of the persons requesting access (or their legal representative, or

both) and data belonging to particular categories as they relate to health (Article 9, paragraph 1, RGPD).

In fact, in most of the accesses, the type of documents requested from the ASL was related to health documentation (including medical records, disability assessments, tests, technical reports, etc.). Furthermore, the field covered by the same registers contained further detailed information relating to the required documentation, also falling within the category of data on the health of the subjects concerned. This considering, for example, that references could be found indicated, depending on the individual case, such as: "XX's visit to the commission of first instance for the assessment of invalidity states"; "Request for acquisition of toxicological analyzes"; "Certified copy of the original clinical examinations, psychiatric visit and psychodiagnostic tests"; "Request for a plain paper copy of the attention function tests"; "[...] delivery of the ultrasound documentation including ultrasound - radiographs and reports of all the examinations carried out from 2009 to 2010"; etc.

As part of the investigation opened in this regard by this Authority, the local health authority Rome 1 confirmed, in its defense briefs, the online disclosure of the personal data described, tracing its conduct to a mere material error due to the circumstance to have uploaded the temporary access file, rather than the definitive one purged of the personal data contained therein.

The ASL declared that it had remedied the situation and had adopted various technical and organizational measures (described in the defense briefs) to correctly publish the documents online, highlighting - in any case - that it had not received any reports from the subjects interested in this regard.

6. Outcome of the investigation

The circumstances highlighted in the defensive writings of the ASL, examined as a whole, although certainly worthy of consideration for the purpose of evaluating the conduct, are not sufficient to allow the filing of this proceeding. This is because, in the case in question, none of the hypotheses provided for by art. 11 of the Guarantor Regulation n. 1/2019.

In this context, the preliminary assessments of the Office are confirmed with the note prot. n. XX of the XX and it is noted that the processing of personal data carried out by the local health authority Roma 1 does not comply with the relevant legislation on the protection of personal data, as the dissemination of personal data contained in the "Access register" received at 'ASL, relating to the years XX and XX, published online (referred to in the files identified above in nos. 1 and 2 of par. 1) occurred in violation:

1) of the prohibition of dissemination of data on the health of interested parties, provided for by art. 2-septies, paragraph 8, of the Code (see also art. 9, paragraphs 1, 2 and 4, of the RGPD);

2) the principle of "minimization" of data, which were not "limited to what is necessary with respect to the purposes for which they are processed" (ie administrative transparency), provided for by art. 5, par. 1, lett. c), of the GDPR;

3) of the provisions contained in art. 7-bis, paragraph 2, of d. lgs. n. 33/2013; of art. 2-ter, paragraphs 1 and 3, of the Code; of the basic principles of the processing contained in the articles 5, par. 1, lett. a) and c); 6, par. 1, lett. c) and e), par. 2 and par. 3, lett. b), of the GDPR; as well as the indications contained in the ANAC Guidelines (det. no. 1309/2016) and in the Circular of the Minister for Public Administration no. 1/2019, referred to above in par. 2.

Considering, however, that the conduct has exhausted its effects, as the data controller has declared that he has remedied his conduct, without prejudice to what will be said on the application of the pecuniary administrative sanction, the conditions for the adoption of further corrective measures pursuant to art. 58, par. 2, of the GDPR.

7. Adoption of the injunction order for the application of the pecuniary administrative sanction (Articles 58, paragraph 2, letter i; 83 of the GDPR)

The Rome 1 local health authority has violated Articles 5, par. 1, lett. c); 6, par. 1, lett. c) and e), par. 2 and par. 3, lett. b); 9, para. 1, 2 and 4, of the GDPR; as well as Articles 2-ter, paragraphs 1 and 3; 2-septies, paragraph 8, of the Code.

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

In the present case, the violation of the aforementioned provisions - also considering the reference contained in art. 166, paragraph 2, of the Code - is subject to the application of the same administrative fine provided for by art. 83, par. 5, of the GDPR, which therefore applies to the case in question.

The Guarantor, pursuant to art. 58, par. 2, lett. i) and 83 of the RGPD, as well as art. 166 of the Code, has the corrective power to "inflict 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 context, "the College [of the Guarantor] adopts the injunction order, with which it also disposes with regard to the application of the ancillary administrative sanction of its publication, in whole or in excerpt, on the website of the Guarantor pursuant to Article 166, paragraph 7, of the Code "(Article 16, paragraph 1, of the Guarantor Regulation no. 1/2019).

The aforementioned administrative fine imposed according to the circumstances of each individual case must be determined in

the amount, taking into 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 is of a negligent nature, deriving from a mere clerical error and involved the online dissemination of personal data for about three years referring to more than a thousand interested parties, including those relating to health (Article 9 of the RGPD). For the purposes of evaluating the conduct, however, the absence of the receipt by the ASL of any reports or complaints from the interested parties, the circumstance - as declared by the ASL - of the possible (even if not proven) absence of "considerable access" to the disputed files, given the plurality of steps that characterized the IT path to access them. It is also taken into account that the data controller, following the request of the Office, intervened promptly, collaborating with the Authority during the investigation of this proceeding in order to remedy the violation, mitigating its possible effects. negative. In the reply to the Guarantor, various technical and organizational measures implemented pursuant to art. 25-32 of the RGPD and, in any case, there are no relevant previous violations of the RGPD committed by the entity.

Due to the aforementioned elements, assessed 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, to the extent of € 46,000.00 (forty-six thousand) for the violation of Articles 5, par. 1, lett. c); 6, par. 1, lett. c) and e), par. 2 and par. 3, lett. b); 9, para. 1, 2 and 4, of the GDPR; as well as art. 2-ter, paragraphs 1 and 3; 2-septies, paragraph 8, of the Code; as a pecuniary administrative sanction deemed effective, proportionate and dissuasive pursuant to art. 83, par. 1, of the same RGPD.

In relation to the specific circumstances of this case, relating to the dissemination of personal data online in violation of the prohibition of dissemination of health data as well as in the absence of a suitable legal basis and in violation of the principle of data minimization, it is also considered that it should be applied the ancillary sanction of the publication of this provision on the Internet site of the Guarantor, 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 out in art. 17 of the Guarantor Regulation n. 1/2019.

WHEREAS, THE GUARANTOR

detected the unlawfulness of the processing carried out by the Local Health Authority of Rome 1 in the terms indicated in the motivation, pursuant to Articles 58, par. 2, lett. i), and 83 of the GDPR

ORDER

to the Local Health Authority of Rome 1, in the person of the pro-tempore legal representative, with registered office in Borgo Santo Spirito, 3 - 00193 Rome (RM) - Tax Code 13664791004 to pay the sum of € 46,000.00 (forty-six thousand) as a pecuniary administrative sanction for the violations mentioned in the motivation;

INJUNCES

to the same Local Health Authority to pay the sum of € 46,000.00 (forty-six thousand), according to the methods indicated in the annex, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the l. n. 689/1981.

Please note that the offender has the right to settle the dispute by paying - again in the manner indicated in the annex - of an amount equal to half of the sanction imposed, within the term referred to in art. 10, paragraph 3, of d. lgs. n. 150 of 1/9/2011 provided for the submission of the appeal as indicated below (Article 166, paragraph 8, of the Code).

HAS

- the publication of this provision on the website of the Guarantor pursuant to art. 166, paragraph 7, of the Code and art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019;

- the annotation in the internal register of the Authority of violations and measures adopted pursuant to art. 58, par. 2, of the RGPD with this provision, as required by art. 17 of the Guarantor Regulation n. 1/2019.

Pursuant to art. 78 of the RGPD, of the arts. 152 of the Code and 10 of the d. lgs. n. 150/2011, against this provision, it is possible to appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the applicant resides abroad.

Rome, May 26, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE DEPUTY SECRETARY GENERAL

Philippi