[doc. web no. 9567489]

Injunction against the Foundation of Religion and Worship "Home for the Relief of Suffering" Opera di San Pio da Pietrelcina - 11 February 2021

Register of measures

no. 46 of 11 February

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by Dr. the professor. Pasquale Stanzione, president, prof. Geneva Cerrina Feroni, vice president, dr. Agostino Ghiglia, the lawyer Guido Scorza, components and Dr. Fabio Mattei, general secretary;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, concerning the protection of natural persons with regard to the processing of personal data, as well as the free movement 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 natural persons with regarding the processing of personal data, as well as the free movement of such data and repealing Directive 95/46/EC (hereinafter the "Code");

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 general secretary 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, doc. web no. 1098801;

Speaker Dr. Agostino Ghiglia;

WHEREAS

1. The personal data breach

On 31 January 2020, the Foundation of Religion and Worship "Casa Relief of Suffering" Opera di San Pio da Pietrelcina

(hereinafter the "Foundation"), with registered office in San Giovanni Rotondo, Viale Cappuccini - VAT number 00138660717, has notified this Authority of a violation of personal data, pursuant to art. 33 of the Regulation. Subsequently, with a note dated February 12, 2020, he supplemented this notification.

In the notification deed, the Foundation stated that the violation concerned the erroneous transmission, by traditional mail, of health documentation to an unauthorized third party.

More specifically, it was a “case of homonymy. The invoice, issued by the Foundation for the cost of sending the postal package, was erroneously attributed to another interested party of the same name (incorrect data: residential address). These (incorrect) data were subsequently used for the composition of the mailing package, by post, of the health report relating to the real person concerned".

In the deed of notification it was also highlighted that the data controller was aware of the violation in question - "(...) materialized on the date of receipt of the envelope by the subject other than the interested party" - on 29 January 2020 , at h. 13.20, following the notification made by the interested party by e-mail.

In describing the cause of the accident, the Foundation explained that "the operator in charge of the composition of the postal package did not verify the correspondence of the personal data on the invoice with those on the health report, identical data for surname and name and different between them only for the residence address” and that the categories of personal data, object of the violation, concern both personal data and data relating to health.

Reference was also made to the technical and organizational security measures adopted to guarantee the security of the data, systems and technological infrastructures involved.

With regard to these measures, adopted following the violation and aimed at both remedying the same and reducing its negative effects and preventing similar incidents from recurring in the future, the Foundation highlighted that:

- "(...) contacts were made (by mail and by telephone) with the interested parties for the adoption of the remedies" and "(...) the postal package was sent to the interested party with the exact data and documents";
- "It has been reiterated to operators who access the IT system and to those involved in the composition of parcels intended for shipment, to consolidate the current practice which provides for verifying the accuracy of data present in the IT systems and in the paper documentation, requesting in the presence of the interested party also the control of the latter at the time of delivery of the documentation "

- the "verification of the processes to support the invoicing for the shipment of reports within the OU involved" was "started".

2. The preliminary investigation.

With note prot. no. 0020108, of 3 June 2020, the Office has requested the Foundation, as data controller, information, pursuant to art. 157 of the Code, in order to receive clarifications in order: to the procedures concerning the sending, by ordinary mail, of the reports requested by the interested parties together with the invoicing of the relative shipping charges; i) the instructions provided to personnel authorized to operate in this phase of the processing of personal data; ii) the methods with which the interested party requested the sending of the report by ordinary mail and, finally, iii) the organizational and technical measures adopted to guarantee the accuracy of the personal data of the patients concerned, with particular reference to those concerning the two procedures mentioned above.

With a note dated June 16, 2020, sent via PEC on June 17, 2020, the Foundation responded to the Authority's request for information, stating that:

- "The dispatch (of the report) can be requested at the time of administrative registration of the health service, or subsequently, referring to the aforementioned outpatient offices. The operators authorized to carry out this procedure are required to check the personal data of the interested party in the computer system; at the same time, the interested party is invited to verify and confirm the same data on the spreadsheets/receipts/invoices delivered. Upon registration of the shipping charges to be paid by the patient concerned, the computer system issues the relative invoice in no. 3 copies: one copy is kept by the branch operator for internal filing purposes; two copies are given to the patient. The same is instructed so that a copy is delivered to the Operating Unit where he will perform the health service while a copy is retained by the interested party, for tax purposes. The copy of the invoice delivered to the Operating Unit is used by the latter to subsequently send it by post";

- "Following the production of the report and its printing, the authorized secretarial operators of the Operating Unit associate the invoice with the report after having carried out the master data control of the two documentary elements, having the computer system as support. The invoice is placed before the sheet(s) that make up the report. The set of sheets is placed in a special envelope with a transparent window displaying the patient's address data. The envelope is closed with an adhesive tab".

The Foundation has also highlighted that:

- healthcare personnel, through operating instructions made accessible on the employee web portal, were made aware of the

incident - even if with reference to different areas than those in question - of the need to pay particular attention to the correct identification of the patient;

- to have "(...) designated its employees as "authorized to process"";

- "annually, at the end of the mandatory Privacy training cycle, these designations are updated".

Based on the elements acquired, the Office, with deed of 7 July 2020 (prot. n. 25124), notified the Foundation, in its capacity as data controller, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the corrective measures pursuant to art. 58, par. 2, of the Regulation, also inviting the latter to produce defense writings or documents to the Guarantor or to ask to be heard by the Authority within 30 days of the request (Article 166, paragraphs 6 and 7, of the Code, as well as Article 18, paragraph 1, of Law No. 689 of 24 November 1981).

In particular, the Office notified that it had ascertained that the Foundation, by mistakenly delivering the health records of another patient to an unauthorized third party, made a communication of health data to third parties in the absence of a suitable legal prerequisite and , therefore, in violation of the art. 9 and of the basic principles of the treatment referred to in articles 5, par. 1, lit. a) and f) of the Regulation.

In the same note, the Office also highlighted that the violation of the aforementioned provisions makes the administrative sanction provided for by art. 83, par.5, lett. a) of the Regulation.

In the context of the proceeding in question, the data controller has not sent the Guarantor written defenses, nor requests for a hearing.

3. Outcome of the preliminary investigation.

Pursuant to the Regulation, personal data must be processed "in a lawful, correct and transparent manner in relation to the data subject" (principle of "lawfulness, correctness and transparency") and "in a way to ensure adequate security of personal data, including the protection, through adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage" (principle of "integrity and confidentiality") - art. 5, par. 1, lit. a) and f) of the Regulation).

As regards, specifically, the health sector, the regulations on the protection of personal data also provide that information on the state of health can only be communicated to the interested party and can 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 Articles 83 and 84 of the Code in the version prior to the reformulation of the same by Legislative Decree 10 August 2018, No. 101 in conjunction with Article 22, paragraph 11, of Legislative Decree No. 101 of 10 August 2018; see also the general provision of 9 November 2005, which can be consulted at www.gpdt.it, web doc. No. 1191411 , deemed compatible with the aforementioned Regulation and with the provisions of decree no. 101/2018; see art. 22, paragraph 4, of the aforementioned legislative decree no. 101//2018).

In particular, the art. 83 of the Code, provides, among other things, that the public and private structures providing healthcare services must adopt "(...) appropriate measures to guarantee, in the organization of services and services, respect for the rights, fundamental freedoms and the dignity of the interested parties, as well as professional secrecy, without prejudice to the provisions of the laws and regulations regarding the methods of processing sensitive data and minimum security measures".

These measures include, in particular:

respect for the dignity of the person concerned during the medical service and in any data processing operation;

the implementation of procedures, including personnel training, aimed at preventing an explicit correlation between the person concerned and departments or structures towards strangers, indicative of the existence of a particular state of health.

In this regard, please also refer to articles 10 to 12 of the Code of medical ethics relating, respectively, to "professional secrecy", "confidentiality of personal data" and "handling of sensitive data".

Furthermore, the Regulation, in sanctioning a general prohibition on the processing of particular categories of data, including those relating to health, admits that they can be processed only in the presence of one of the conditions referred to in art. 9, par. 2 (see in particular, article 9, paragraph 2, letters a), g), h) and i)).

Having acknowledged what is represented by the Foundation in the documentation in the file, it is noted that the latter, by mistakenly delivering the health documentation of another patient to an unauthorized third party, communicated health data to third parties in the absence of a suitable legal basis, in violation of the aforementioned principles and regulatory provisions.

4. Conclusions.

In the light of the assessments referred to above, taking into account the statements made by the owner during the investigation - and considering that, unless the fact constitutes a more serious crime, anyone who, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances o produces false deeds or documents and is liable pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the duties or exercise of the

powers of the Guarantor" as well as in the absence of further documentation and defense briefs that the holder could have produced within the legal term indicated in the deed of initiation of the procedure for the adoption of corrective measures pursuant to art. 58, par. 2 of the Regulation, the findings notified by the Office with this last deed are confirmed, since none of the cases provided for by art. 11 of the Regulation of the Guarantor n. 1/2019.

For these reasons, confirming the preliminary assessments of the Office, the unlawfulness of the processing of personal data carried out by the Foundation of religion and cult "Casa Relief of Suffering" is noted in the terms set out in the justification, since, the successful shipment of a package containing medical documentation to a third party, not authorized to receive such documentation, rather than to the interested party, has resulted in a communication of data relating to health in the absence of suitable legal conditions (article 9 of the Regulation and articles 83 and 84 of the Code in conjunction with Article 22, paragraph 11, Legislative Decree No. 101 of 10 August 2018), with consequent violation of the basic principles applicable to the processing, in particular, those referred to in Article 5, par. 1, lit. a) and f) of the Regulation.

In this context, considering, however, that the conduct has exhausted its effects - also expected that the Foundation has declared that the interested parties have been contacted by post and by telephone and the postal package has been sent to the interested party with the exact data and documents - the conditions for the adoption of further corrective measures by the Authority, 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; article 166, paragraph 7, of the Code).

The violation of the articles 5, par. 1, lit. a) and f), and 9 of the Regulation, determined by the processing of personal data, subject of this provision, carried out by the Foundation, is subject to the application of the administrative fine pursuant to art. 83, par.5, lett. a) 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 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 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 violation concerned only one interested party, a patient of the Foundation (Article 83, paragraph 2, letter a) of the Regulation);
- the episode appears to have been unique and isolated, not malicious, due to the fault of an operator, an employee of the Foundation, also determined in the face of a case of homonymy concerning two patients of the same Foundation (art. 83, par. 2, lett b) of the Regulation);
- the Authority became aware of the event following the personal data breach notification made by the data controller himself (Article 83, paragraph 2, letter h) of the Regulation);
- the data controller promptly took action to remedy the incident through postal and telephone contacts with the interested parties, as well as intervening on the technical and organizational measures to guarantee the correctness of the billing process (Article 83, paragraph 2, letter c) and d) 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 Regulation, to the extent of 5,000 (five thousand) euros for the violation of articles 5, par. 1, lit. a) and f) and 9 of the Regulation as a pecuniary administrative sanction, 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.

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

found the violation of the articles 5, par. 2, lit. a) and f), and 9 of the Regulation, declares the unlawfulness of the processing of personal data carried out by the Foundation in the terms set out in the justification;

ORDER

to the Foundation of Religion and Worship "Casa Relief of Suffering" Opera di San Pio da Pietrelcina, with registered office in San Giovanni Rotondo, Viale Cappuccini – VAT number 00138660717, in the person of its legal representative pro-tempore, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to pay the sum of 5,000.00 (five thousand) euros as an administrative fine for the violation referred to in this provision, according to the methods indicated in the attachment, within 30 days of the notification in the justification; 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 health facility, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of 5,000.00 (five 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 deeds pursuant to art. . 27 of the law n. 689/1981.

HAS

the publication of this provision on the Guarantor's website, pursuant to art. 166, paragraph 7, of the Code;

annotation of this provision in the internal register of the Authority - provided for by art. 57, par. 1, lit. u), of the Regulation, as well as by 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 - relating to violations and measures adopted in compliance with art. 58, par. 2, of the same Regulation.

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