[doc. web n. 9688020]

Injunction order against ATS of Bergamo, Health Protection Agency - May 13, 2021

Record of measures

n. 206 of May 13, 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stazione, president, Professor Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, members, and the cons. Fabio Mattei, general secretary;

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

GIVEN the legislative decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national system to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of individuals with regard to to the processing of personal data, as well as to the free circulation of such data and which repeals Directive 95/46 / EC (hereinafter the "Code");

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");

Having seen 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. The violation of personal data

With a note dated 1 March 2019, the ATS of Bergamo, Health Protection Agency (hereinafter ATS or Agency) notified the

Guarantor of a violation of personal data, pursuant to art. 33 of the Regulations, consisting in the forwarding, for the compilation of a questionnaire of "(...) three emails with multiple recipients (each having 62 recipients). Despite precise instructions given to the operator in charge of sending, the email addresses of each group of recipients have been entered in the (...) Cc field, instead of in the (...) Ccr / Bcc field. In this way, those who received the email became aware of the email addresses of the other 61 recipients of the communication. From the text of the email it emerges that the recipients of the communications are people (or, more often they are family members of people) who suffer from developmental disorders with particular reference to autism spectrum disorders. (...) It cannot therefore be ruled out that those who received the email will be able to trace the precise identity of other recipients, thus indirectly gaining knowledge (...) even of a data relating to health ".

2. The preliminary activity

With reference to the aforementioned violation, as part of the preliminary investigation launched by the Office of the Guarantor, the Agency with a note dated 29 January 2021 (prot. of 30 December 2020, prot.

"On February 28, 2019, on (...), director of the Department of Planning for the Integration of Social and Health Services with Social Services (DPIPSS), following the episode of violation of personal data that took place on the same day (...), summoned for the following day, 1 March 2019, Mr. (...), in charge of sending the emails, to a meeting (...) ";

On that occasion, the person in charge of sending the recalled emails was highlighted "the seriousness of what happened due to the failure to apply the instructions received (...) on the use of the" CCN "method for sending the email containing the customer satisfaction form intended for people with autism spectrum disorders and / or their families ";

the DPIPSS director "on March 6, 2019, convened a meeting of the Department staff for March 11, 2019 in order to share what happened, explaining its dynamics, and then proceed with the rereading of the Operating Instructions (...) dedicated to "Workstation and network services". The meeting was attended by all 20 guests belonging to the DPIPSS, as can be seen from the signature collection sheet. The minutes of the meeting show that during the meeting the need for a clearer and more explicit formulation of the procedure concerning the sending of communications by e-mail emerged. This need was shared by the Manager of the Legal and Insurance Affairs Area who then submitted it on 12 March 2019 to the head of the procedure (...), manager of the Corporate IT Services (SIA) for a review ";

"The new Operating Instruction (...) issued on May 15, 2019 and published on the Company bulletin board on May 20, 2019 reports in chap. 3, paragraph 3, the detailed rules relating to the sending of emails containing sensitive data and, in particular,

precise indications on the use of the "CCN" (blind carbon copy) field in the case of multiple recipients ";

"The Data Protection Officer of the Bergamo ATS (...) who was immediately notified of the" data breach "episode on the same evening of February 28, 2019, supported the Bergamo ATS in the whole affair and, in the updating and training meetings of April 18, 2019 and May 20, 2019, he addressed the problem with the privacy contacts of the ATS ";

«To date, this ATS has not received written complaints from any of the recipients of the emails sent. Conversely, in the immediacy of the episode, two phone calls were received from families resentful of the incident, to which the necessary apologies were given ";

"For the sake of completeness of information, it should be noted that the disciplinary sanction of written reprimand was imposed on the employee in charge of sending the emails".

On the basis of the elements acquired, through the communication of the violation of personal data as well as in the context of the preliminary investigation, the Office, with deed dated February 16, 2021 prot. n. 9375, notified on the same date by certified e-mail, which here must be understood as fully reproduced, has initiated, pursuant to art. 166, paragraph 5, of the Code, with reference to the specific situations of illegality referred to therein, a procedure for the adoption of the measures referred to in art. 58, par. 2 of the Regulation, against the same Agency inviting it to produce defensive 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, l. N. 689 of 24 November 1981).

With a note dated 12 March 2021 (prot. No. 25922), the Agency sent its defense briefs providing the elements referred to in art. 83, paragraph 2 of the Regulation, in which, in particular, it was represented that:

a) in relation to the disputed fact and event "With regard to the number of subjects involved in the violation, it is worth emphasizing first of all that since the sending was divided into 3 groups of 62 recipients each, the maximum number of addresses" known "by each recipient was limited to 61 units (instead of the 185 possible in the case of a single mailing) "; moreover, only a hundred email addresses (out of a total of 186) report a name and surname as an “account” (…). The remaining email addresses report as "account" either only a name, or only a surname, combined or not in numbers, or invented names, and in these cases the possibility of tracing the real identity of the recipient seems very remote ";

b) in relation to the subjective elements of the conduct: "The violation is to be considered culpable due to the negligence of the employee sending the mail, who was expressly indicated to enter the addresses of the recipients in the CCN field";

c) with reference to the measures adopted to mitigate the effects of the violation for the interested parties "On the same day in which the violation occurred, the parties involved (...) were sent, again by e-mail, a communication of apology by which the error that occurred is explained. In some cases, the recipients' email addresses were found to be inactive or incorrect; the people who for this reason did not receive the email intended for them were in any case contacted by paper mail and / or by telephone in order to be adequately informed of the incident ";

d) with reference to the technical and organizational measures put in place by the Data Controller in general and following the notification of data breach: "In replacement of the Operational Instruction (...) issued on 7 November 2017 and in force at the time of the violation, it was issued on 15 May and a new Operating Instruction was published on the Company notice board on 20 May 2019, (...) which, in chap. 3, paragraph 3, contains the detailed rules relating to the sending of emails containing sensitive data and, in particular, precise indications on the use of the "CCN" (blind carbon copy) field in the case of multiple recipients. On April 18 and May 20, 2019, meetings were held by the DPO (DPO) to update and train the privacy representatives of the ATS during which the problem that emerged during the violation was addressed. Together with the DPO, actions are implemented to monitor the procedure defined by the Company described above ";

e) "An awareness campaign has been launched through training meetings for employees on the subject of Data Protection and in particular on the use of the IT tools in use";

The Agency therefore asked this Authority to favorably assess "the timeliness with which the violation was communicated, the immediate involvement of the DPO, the transparency with which the subjects involved were made aware of the violation , the limited number of subjects involved also due to the method of sending adopted, the (in) training activity promptly implemented by the ATS and the DPO which involved and the Agency's privacy contacts ".

3. Outcome of the preliminary investigation

As a preliminary point, it should be noted that "personal data" means "any information concerning an identified or identifiable natural person (" data subject ")" and "data relating to health" "personal data relating to the physical or mental health of a natural person, including the provision of health care, which discloses information relating to his state of health "(Article 4, paragraph 1, nos. 1 and 15 of the Regulation). Therefore, the information subject of the notification, contained in the aforementioned emails, which attached a questionnaire addressed to families with people suffering from autism spectrum disorders in order to detect the satisfaction of the interventions they use, constitute personal data relating to health (cf. ., on the

traceability of the email address to the notion of personal data, formerly Provv. 25 June 2002, web doc. no. 29864 and Provv. of 9 January 2020, web doc. 9261234).

With particular reference to the question raised, it should be noted that personal data must be "processed lawfully, correctly and transparently" (principle of "lawfulness, correctness and transparency") and "in order to guarantee adequate security (...), including the protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage (principle of "integrity and confidentiality") "(Article 5, paragraph 1, letter a) and f) of the Regulation).

The regulation on the protection of personal data provides - in the health sector - 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 basis or on the indication of the interested party. subject to written authorization from the latter (Article 9 of the Regulations and Article 83 of Legislative Decree No. 196 of 30 June 2003 (Code regarding the protection of personal data - hereinafter the "Code") in conjunction with 'Article 22, paragraph 11, legislative decree 10 August 2018, n.101; see also general provision of 9 November 2005, available at www.gpdt.it, web doc. n. 1191411, deemed compatible with the the aforementioned Regulation and with the provisions of decree n.101 / 2018; see art.22, paragraph 4, of the aforementioned legislative decree n.101 / 2018).

Given the above, with regard to the present case, the Agency confirmed, in the defense briefs the fact that from the context of the communication sent with the aforementioned e-mails it could be inferred that the recipients of the same, "are people (or, more often they are family members of persons) who suffer from developmental disorders with particular reference to autism spectrum disorders (...) "and that therefore such communications concerned information relating to health, as such subject to the regulations on the protection of personal data. In particular, this communication involved the processing of personal data in violation of the provisions ascertained by the Guarantor with a note dated 16 February 2021 prot. n. 9375 even if caused by culpable conduct "due to the negligence of the employee who sent the mailing, who was expressly instructed to enter the addresses of the recipients in the CCN field".

The Agency also stressed that following the incident "a new Operating Instruction, IOIT05-5) was issued on May 15 and published on the Company bulletin board on May 20, 2019. 3, paragraph 3, contains detailed rules relating to the sending of e-mails containing sensitive data and, in particular, precise indications on the use of the "CCN" field "and to have implemented

specific measures described above to mitigate the effects of the violation in towards the interested parties.

4. Conclusions

In light of the aforementioned assessments, taking into account the statements made by the owner during the investigation the truthfulness of which one may be called to answer pursuant to art. 168 of the Code the elements provided by the data controller in the defense brief, although deserving of consideration, do not allow to overcome the findings notified by the Office with the act of initiating the procedure, however, none of the cases provided for by the art. 11 of the Guarantor Regulation n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the ATS of Bergamo, Health Protection Agency, is noted for having communicated data relating to the health of 186 patients, in the absence of a suitable legal basis and, therefore, in violation of the basic principles of the processing referred to in art. 5, par. 1 letter a) and f) and 9 of the Regulations as well as art. 75 of the Code, which summarizes the conditions for the processing of personal data for the purpose of protecting health in the health sector.

The violation of the aforementioned provisions makes the administrative sanction provided for by art. 83, par. 5 of the Regulations, as also referred to by art. 166, paragraph 2, of the Code, pursuant to art. 58, par. 2, lett. i) of the Regulations.

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, no the conditions for the adoption of measures, of a prescriptive or inhibitory nature, pursuant to art. 58, par. 2 of the Regulations.

5. Adoption of the injunction order for the application of the pecuniary administrative sanction and ancillary sanctions (articles 58, par. 2, lett. I and 83 of the Regulation; art. 166, paragraph 7, of the Code).

The violation of art. 5, par. 1, lett. a) and f) and 9 of the Regulations as well as art. 75 of the Code, caused by the conduct put in place by the Bergamo ATS Agency is subject to the application of the administrative fine pursuant to art. 83, par. 5, lett. a) (see Article 166, paragraph 2 of the Code).

The Guarantor, pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, has the power to "inflict an administrative pecuniary 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 each single case "and, 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, 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 light of the elements provided for in art. 83, par. 2 and of the Regulation, in relation to which it is noted that:

1. the data processing carried out concerned information suitable for detecting the state of health of n. 186 particularly vulnerable subjects as they were people (or, more often, family members of people) who suffer from autism spectrum disorders, (art.4, par.1, n.15 of the Regulation and art.83, par. 2, letters a) and g) of the Regulation);

2. the Authority became aware of the violation through the notification of the violation of personal data carried out by the Agency on 1 March 2019 and no reports or complaints were received regarding the conduct covered by this proceeding; Furthermore, there are no previous relevant violations committed by the data controller, nor have any measures previously been ordered pursuant to art. 58 of the Regulation;

3. the conduct, while not having the character of intentionality, is characterized by gross negligence, taking into account that the employee "was expressly instructed to enter the addresses of the recipients in the CCN field";

4. the data controller, as soon as he became aware of the violation, has put in place specific measures to mitigate the effects of the violation for the interested parties and has adopted organizational measures aimed at avoiding the repetition of the unlawful conduct, providing for:

the integration of the Operating Instruction which indicates in a specific section the rules to follow when sending emails containing sensitive data and, in particular, precise indications on the use of the "CCN" (blind carbon copy) field in the case of multiple recipients;

the meeting by the Data Protection Officer for updating and training the privacy contacts of the ATS during which the problem that emerged during the violation was addressed.

actions to monitor the aforementioned operating procedure.

6. the Agency collaborated promptly with the Authority, during the investigation and this proceeding;

Due to the aforementioned elements, assessed as a whole, it is believed to determine the amount of the pecuniary sanction provided for by art. 83, par. 5, lett. a) of the Regulations, to the extent of € 20,000 (twenty thousand) for the violation of Articles 5, par. 1, lett. a), f) and 9, of the Regulations and art. 75 of the Code, as a pecuniary administrative sanction, pursuant to art. 83, par. 1 and 3 of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary sanction of the publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Guarantor Regulation n. 1/2019, also in consideration of the type of personal data subject to unlawful processing.

Finally, it is noted that the conditions set out in art. 17 of Regulation no. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

WHEREAS, THE GUARANTOR

declares the unlawfulness of the processing of personal data carried out by ATS di Bergamo, Health Protection Agency, for the violation of Articles 5, par. 1, lett. a), f) and 9 of the Regulations and art. 75 of the Code in the terms set out in the motivation.

ORDER

pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, ATS of Bergamo, Health Protection Agency, with registered office in Bergamo, Via Gallicciolli 4 - VAT number: 04114400163, in the person of the pro-tempore legal representative, to pay the sum of € 20,000.00 (twenty thousand) as a pecuniary administrative sanction for the violations indicated in this provision.

It is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, of an amount equal to half of the sanction imposed 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.

INJUNCES

to the aforementioned Agency, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 20,000.00 (twenty 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 law n. 689/1981.

HAS

pursuant to art. 166, paragraph 7, of the Code, the full publication of this provision on the website of the Guarantor and believes that the conditions set out in art. 17 of Regulation no. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

Pursuant to art. 78 of the Regulation, of art. 152 of the Code and 10 of Legislative Decree no. 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 13, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei