[doc. web n. 9722297]

Injunction order against the University Hospital of Modena - September 16, 2021

Record of measures

n. 328 of 16 September 2021

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 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;

Speaker prof. Pasquale Stanzione;

WHEREAS

1. The violation of personal data.

With a note dated the XXth, the University Hospital of Modena notified a violation of personal data, declaring that "out of nine

e-mails sent to CCN regarding the invitation to fill in a questionnaire on the state of health by patients, one is was sent to 98 addresses (out of 1456) in CC: instead of CCN. The questionnaire is aimed at gathering information to provide assistance to HIV patients followed by the Infectious Diseases Outpatient Clinic of the University Hospital of Modena, two months after the interruption of scheduled outpatient visits, due to COVID-19 ".

In the aforementioned communication it was highlighted that the violation concerned contact data and health data and that the 98 interested parties, in communicating the violation, were asked not to disclose their e-mail addresses and to cancel the e-mail received. It was also specified that "the sending of e-mails in the manual mode described above was an occasional event, linked to the need to reorganize the post-COVID-19 outpatient visits of a company specialist clinic and will not be repeated in the future . Automatic systems will be set up for the eventual sending of massive emails, which prevent errors related to the manual 'copy-paste' mechanism ".

2. The preliminary activity.

In relation to what was communicated by the Company, the Office, with deed of XX prot. n. XX, 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, towards the same Company, 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 November 24, 1981).

In particular, the Office, in the aforementioned deed, has preliminarily represented that:

- the information subject of the notification constitutes personal data relating to health (cf., on the traceability of the e-mail address to the notion of personal data, formerly Provv. 25 June 2002, available at www.gpdt.it, web doc. n. 29864);
- the rules on the protection of personal data provide - 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 (Article 9 of the Regulation and art.84 of the Code in conjunction with art.22, paragraph 11, legislative decree 10 August 2018, n.101);
- the legislator has provided for enhanced protection for the processing of data relating to HIV infection, providing, on the one hand, the obligation to communicate the results of direct or indirect diagnostic tests for the aforementioned infection to the only person to whom such tests are carried out on the other hand, they refer to the obligation, on the part of the health care worker

and of any other person who becomes aware of a case of AIDS or HIV infection, to adopt any measure or device for the protection of the rights of the person and of his dignity (art. 5, paragraph 4 and art. 1, paragraph 2, law 5 June 1990, n. 135).

The aforementioned regulatory provisions fall within the specific sector provisions without prejudice to 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 data controller is, in any case, required to comply with the principles of data protection, including that of "integrity and confidentiality", according to which personal data must be "processed in such a way as to guarantee adequate security (...), including protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage "(Article 5, paragraph 1, letter f) of the Regulation) .

Having said this, on the basis of the elements in the file, with the aforementioned note of the XXth, the Office has deemed that the Company, by entering the address of the 98 recipients of the e-mail - with which patients affected by HIV followed by the Infectious Diseases outpatient clinic were invited to fill in a questionnaire on their state of health - in the field called "knowledge copy" it allowed, in fact, all recipients of the aforementioned communication to know the e-mail address of others HIV-infected subjects under treatment at the same clinic. Therefore, the same Company made a communication of data relating to the health and, in particular, HIV infection, of 98 patients to as many patients, in the absence of a suitable legal basis and, therefore, in violation of the basic principles of the treatment of referred to in Articles 5 and 9 of the Regulations as well as art. 75 of the Code.

With a note from the twentieth century, the Company sent its defense briefs, with attached documentation, in which, in particular, it was represented that:

a) in relation to the disputed fact and event "it should be noted that among the 98 e-mail addresses, over half (about 50) are addresses without references to the name and surname or in any case to other data directly identifying the data subjects. In any case, the aforementioned e-mail did not contain any further personal data of the interested parties, with the exception of the information, which can be inferred from the context of the communication, that the recipients were "users of the metabolic clinic / clinic of the AOU of Modena" and that they were "followed by an Infectious Disease Doctor" ";

b) "the purpose of the processing described in the previous paragraph was to provide health care and therapy to the recipients of the e-mail in question, in compliance with art. 9, 2nd paragraph, lett. h) of the Regulations "; "The national emergency context characterized by the well-known COVID-19 pandemic, had forced the Company to adopt methods of communication

with users, replacing the periodic visits normally practiced to the patients in question, unexpected and unpredictable at the time in which it was the design of the treatment is defined. The design of the treatment did not in fact provide for the sending of questionnaires via e-mail to the patients under examination. In the present case, in fact, in the exceptional context and unprecedented emergency for the country, the Company was forced to temporarily suspend the planned treatment and assistance paths and the questionnaire sent via the attached e-mail was intended to identify those patients who, due to the aforementioned suspension, presented critical situations. Through the questionnaire, in particular, the Company aimed to schedule the visits based on the clinical priorities of the patients, acquiring information on the state of health of the latter under treatment with alternative methods to those ordinarily provided for an outpatient visit, submitting " remotely ”the questionnaire that can be filled out on the link contained in the e-mail. The aforementioned e-mail was therefore sent in a totally exceptional way, outside the procedures that the Company had given itself in planning the processing of personal data, for the sole purpose of fulfilling, during the COVID-19 emergency, to - urgent and not postponable - remote care and health care commitments, in an exhausted operational context and notoriously close to collapse for many Italian regions ";

c) "as far as the Company is aware, the communication in question, certainly of a generic content, did not cause any harm to the interested parties. This must be assumed from the fact that out of 98 patients affected by the alleged violation, more than two months after the communication to the interested parties pursuant to art. 34 of the Regulations, only one patient had filed a telephone complaint with the Company on the date of submission of these defensive writings ";

d) in relation to the subjective elements of the conduct, in the period in dispute, due to the Covid19 emergency, "all offices and departments (..) were burdened with extreme working hours, well beyond the usual overtime that can sometimes be required in temporally limited situations. This also concerned the IT office from which the e-mail was sent, called upon to IT support the timely reorganization of hospital departments and local structures for better emergency management. (...), concluding that "although the alleged violation originates from a human error (the insertion of addresses in the wrong string), the context of absolute exceptionality and emergency in which the Company was operating excludes the existence of the element of fault required by the reference standards for the purposes of punishing the conduct and therefore the imposition of any sanctions. The state of emergency that in those days characterized the working environment in an absolutely exceptional way, professionally as well as emotionally exhausting and exhausting, leads to the argument that the exemption of force majeure can be considered operative. The latter is not exhausted in a single isolated fact or event, but in the persistence - constant and

protracted over time - of the state of epidemic. Despite having adopted adequate safety measures of an organizational and technical nature, the Company was unable to avoid the event in question, given that the unexpected need to deal with the epidemic had forced the department concerned to identify methods of treatment and health assistance. of the relative patients, alternatives to the usual and planned examination and control tools. From this unforeseen need came the massive (isolated and exceptional) sending of the group of e-mails containing the link of the questionnaire to patients affected by the human immunodeficiency virus, which, precisely due to the peculiarity of the pathology, required a form of health assistance and control also in the aforementioned emergency period. (…). In terms of administrative sanctions, even if they are not expressly mentioned by the law of 24 November 1981, n. 689, the jurisprudence considers with a consolidated orientation that the fortuitous event and force majeure must be considered implicitly (Cass. Civ., Section II, 29 April 2010, n. 10343) included in the provision of art. 3 of the law itself and exclude the agent's liability, both affecting guilt and force majeure on the psychic link. The orientation is shared by the prevailing doctrine (...), according to which the cause of force majeure and the fortuitous event constitute "statutory hypotheses of abnormal circumstances, which prevent the agent from conforming his behavior to the objective rule of diligence to be observed in the concrete case ". According to this doctrine, fortuitous events and force majeure therefore constitute “legally typified excusing circumstances” which “affect the same punishment” (….). The above considerations therefore lead to consider the Company's conduct in the specific context not punishable, resulting in an exclusion of the data controller's liability due to force majeure ";

e) with reference to the measures adopted to mitigate the effects of the violation for the interested parties, "immediately after the alleged violation, the Company sent an e-mail to all interested parties an apology (...) dated XX, asking the individual users (in blind carbon copy mode) to delete the previous e-mail ";

f) with reference to the technical and organizational measures put in place by the Data Controller in general and following the notification of data breach: "all the IT equipment supplied to the Company is protected by adequate antivirus and firewall systems, as well as by (..)" specific “technical security measures (…). The e-mail server located inside the Company's data center is also equipped with antivirus, using an antispam system called Trend Micro equipped with a sandbox "(...); "Following the occurrence of the alleged violation in question, in order to avoid that a human distraction could lead to a possible data violation in the future, the mass sending of e-mails was inhibited, as occurred exceptionally in the case of species. In particular, we intervened on the software used, called LimeSurvey, so that, given a list of e-mail addresses to which the same

communication is to be addressed, a single e-mail is prepared for each recipient, effectively eliminating the mass sending functionality. of the same e-mail to multiple recipients, even with "carbon copy" mode. The aforementioned LimeSurvey program interfaces with the Zimbra e-mail program, in order to transmit as many individual e-mails as there are individual recipients of the communication, so that no recipient can view any further e-mail addresses of third parties ".

The Company therefore requested that the archiving request be accepted or, in the alternative, that the alleged violation be ascribed to the mere slight negligence of the owner, with every consequence on the commensuration of the sanction, or, in any case, that the any provision of the Authority is limited to a purely prescriptive content.

3. Outcome of the preliminary investigation.

Having taken note of what the Company represents in the defense briefs, it is noted that:

- considering that "personal data" means "any information concerning an identified or identifiable natural person (" interested ")" (Article 4, paragraph 1, no. 1 of the Regulation), the e-mail addresses, as already highlighted in the note of the XX, are attributable to the notion of personal data; therefore, even if half of the e-mail addresses were devoid of references to the name and surname or in any case to other data directly identifying the data subjects, it is personal information, subject, like the others, to the application of the regulations on personal data protection;

- the circumstance that from the context of the communication it could be inferred that the recipients of the same were "users of the metabolic clinic / clinic of the AOU of Modena" and that they were "followed by an Infectious Disease Doctor", implies that the treatment, with respect to which it is the data breach notification was sent to the Guarantor, it concerned information relating to health, given that, for this category of data, we mean "personal data relating to the physical or mental health of a natural person, including the provision of health care, which reveal information relating to your state of health "(Article 4, paragraph 1, no. 15 of the Regulation);

- as regards the request to evaluate the exclusion of the subjective element, motivated on the assumption of the occurrence of a circumstance of force majeure materializing "in the persistence - constant and protracted over time - of the state of epidemic", it should be noted that, in order to the recurrence of the case of force majeure can be recognized, it is necessary, according to the orientation of the jurisprudence, that the realization of the event itself, or the consummation of the unlawful conduct, is "due to the absolute and innocent impossibility of the agent to comply to the juridical command (..) The force majeure excludes, as is known, the suitas of the conduct, constituting the reason why the man "non agit sed agitur" (Cass.,

Section VII, 8 March 2019, n.14789) . According to the constant jurisprudence of legitimacy, force majeure is the exclusive cause of the event, not instead as a concurrent cause of it (Cass., Section IV, November 23, 1982, n. 1492). (...) Force majeure, in fact, postulates the verification of an unforeseen and unforeseeable fact, such as to make the occurrence of the event inevitable and which cannot be connected in any way to a conscious and voluntary action or omission of the agent "(see, lastly, Cass . Criminal, Section 3, no. 15218/2020). In the case in question, the exceptional nature of the circumstances deriving from the health emergency which, as is well known, made the carrying out of the working activity exhausting both from a professional and emotional point of view, if they justify, as described, the need for resorting to a different treatment method, compared to the usual and programmed visit and control tools - which, according to the Company, determined a "massive (isolated and exceptional) sending of the group of e-mails containing the link of the questionnaire to patients affected by the human immunodeficiency virus, who, precisely due to the peculiarity of the pathology, required a form of medical assistance and control even in the emergency period "- does not allow us to believe that an event has occurred such as to objectively prevent not so much the aforementioned dispatch in a massive way of the communication concerning the questionnaire, as the insertion of the address of all the recipients of the email in the cam bit called "carbon copy", in place of the field "blind carbon copy" (Cf. on this point, also the FAQ n. 2 on "Data processing in the health context in the context of health emergencies", available at www.gpdt.it, doc. web n. 9293264, in which it is highlighted that, in the event that the healthcare company uses e-mail to communicate at the same time to all subjects the provisions that are required to observe, for example, during the quarantine period, it must take care to enter the " address of the e-mail recipients in the field called "blind carbon copy" (bcc), in order to prevent all recipients of the aforementioned communication from being aware of the e-mail address of the other subjects).

Therefore, assuming that, unless the fact constitutes a more serious crime, anyone, 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 ("False statements to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor"), following the examination of the documentation acquired as well as the statements made to the Authority during the procedure, and in light of the aforementioned assessments, the elements provided by the data controller in the defense briefs do not allow to overcome the findings notified by the Office with the act of initiation of the procedure, since none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the University Hospital of Modena, for having made a communication of data relating to health and, in particular, HIV infection, of 97 patients to as many patients, is detected, in the absence of a suitable legal basis and, therefore, in violation of the basic principles of the processing referred to in Articles 5 and 9 of the Regulations as well as art. 75 of the Code, which summarizes the conditions for the processing of personal data for health protection purposes in the health sector, recalling the specific sector provisions. Among these, in the specific case, we highlight the obligation, on the one hand, to communicate the results of direct or indirect diagnostic tests for HIV infection to the only person to whom these tests refer, on the other hand, the obligation, for the health worker and any other person who becomes aware of a case of AIDS or HIV infection, to take all measures or precautions for the protection of the rights of the person and his dignity (Article 5, paragraph 4 and art. 1, paragraph 2, law 5 June 1990, n. 135).

In this context, considering, in any case, that the conduct has exhausted its effects, the conditions for the adoption of the corrective measures referred to in art. 58, par. 2, of the Regulation.

4. 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. f) and 9 of the Regulations as well as art. 75 of the Code, caused by the conduct put in place by the University Hospital of Modena, is subject to the application of a pecuniary administrative sanction 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. 85, par. 2 and of the Regulation, in relation to which it is noted that:

- the data processing carried out concerned information, suitable for detecting the state of health, in particular, relating to HIV infection, for which the legislator has provided for enhanced protection; the subjects involved are 98 (art. 4, par. 1, n. 15 of the Regulations and art. 83, par. 2, letters a) and g) of the Regulations);

- even considering the smallness of the complaints presented to the Company, at the time of the presentation of the defense writings, by the subjects whose data have been communicated (only one case), it is not possible to exclude that they may have suffered, o suffer in the future, prejudicial consequences for the effect of the Company's conduct, especially in consideration of the fact that they are vulnerable subjects as information relating to their state of health and, in particular, concerning infection by HIV (Article 83, paragraph 2, letter a) of the Regulation);

- the Company promptly collaborated with the Authority, during the investigation and, in apologizing to the interested parties for the incident, asked them not to disclose the other e-mail addresses and to delete the e-mail received (art 83, par. 2, letters c) and f) of the Regulation);

- it was the Healthcare Company itself that communicated the aforementioned communication of personal data to the Guarantor, through the notification of personal data violation (Article 83, paragraph 2, letter h), of the Regulation);

- the Company has adopted organizational measures aimed at avoiding the repetition of the unlawful conduct, inhibiting the massive sending of emails and providing for the use of software which, from a list of email addresses to which the same communication is to be sent, prepare a single e-mail for each recipient (Article 83, paragraph 2, letter c), of the Regulation);

- the violation is culpable and the conduct arose in the context of the peculiar working context characterized by strong stress and fatigue of the operators due to the persistent emergency context deriving from the Covid-19 epidemic, which strongly affected the company concerned (art . 83, par. 2, letters b) and k)).

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. f) and 9, of the Regulations and art. 75 of the Code which is without prejudice to the specific provisions of the sector, including law no. 135/1990 (containing the "Plan of urgent interventions in the field of prevention and fight against AIDS"), 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 potential number of interested parties and 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 the University Hospital of Modena, for the violation of Articles 5, par. 1, lett. 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, to the University Hospital of Modena, with registered office in Modena, Via del Pozzo 71 - VAT number: 02241740360, 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 Company, 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, September 16, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Stanzione

THE DEPUTY SECRETARY GENERAL

Philippi