[doc. web no. 9861356]

Injunction against the Padua University Hospital Company - January 11, 2023

Register of measures

no. 7 of 11 January 2023

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

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

HAVING REGARD TO Legislative Decree 10 August 2018, n. 101 containing "Provisions for the adaptation of national legislation to the provisions of 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 circulation of such data and repealing Directive 95/46/EC";

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

HAVING REGARD to the documentation in the deeds;

HAVING REGARD TO 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 Guarantor's office for the protection of personal data, doc. web no. 1098801;

Speaker the lawyer Guido Scorza;

WHEREAS

1. The personal data breach

On the 20th date, the Padua University Hospital (hereinafter the "Company") notified the Authority, on a preliminary basis, of a violation of personal data, pursuant to art. 33 of the Regulation, representing, in particular, that "as part of the acquisition of informed consent for participation in a clinical study (UOC Cardiac Surgery) an email was accidentally sent (...) to patients involved in the clinical study in which the their address book was sent not in ccn (blind copy) but in cc (carbon copy) thus making the e-mail address of all patients awaiting heart transplantation unintentionally known and who, in the preliminary phase, gave their consent to the treatment of your personal data".

In relation to this event, it was also declared that the subjects involved in the violation are 19 and that "there is an updated Regulation for the use of IT tools, e-mail and the Internet of the Padua University Hospital adopted with resolution no. XX of the XX, communicated to all directors of UOC and UOSD and sent to the email of all staff. With previous resolution no. 262 of 7/3/2019, among other things, the operating instructions that the Privacy Delegates must impart to the personnel of the structure under their responsibility have been adopted. Over time and still today, training courses have been carried out for all staff".

To remedy the violation and reduce its negative effects for the interested parties, a "communication was made to the company DPO and instructions were given to the Director of the Cardiac Surgery UOC to inform each individual interested party of the error via e-mail, recommending that the previously sent e-mail be deleted with the unencrypted address book and not to use said email addresses".

In relation to the technical and organizational measures whose adoption is proposed to prevent similar future violations, the intention was represented to "instruct the Director of the concerned UOC, as privacy delegate, to make personnel aware of the attention in the place before sending communications to several interested patients (according to what is already provided for in the operating instructions mentioned above)".

With subsequent communication of the XX, in integrating the aforementioned notification, made on the XX, the Company confirmed what has already been declared, highlighting that the seriousness of the potential impact for the interested parties is medium, considering that "the health data (pending heart transplant) is isolated and common to all those involved" and "is not

accompanied by any other sensitive data".

2. The preliminary investigation

With regard to the case described, the Office, on the basis of what was represented by the Company in the deed of notification of the violation (preliminary and supplementary), as well as subsequent assessments, notified the aforementioned data controller, pursuant to art. 166, paragraph 5, of the Code, the initiation of a procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation, inviting him to produce written defenses 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, of law n. 689 of the 11/24/1981). In particular, with deed n. XX of the XX, the Authority considered that the Company had communicated data relating to health in the absence of a suitable legal prerequisite, in violation of the basic principles of treatment pursuant to articles 5, 6 and 9 of the Regulation and of the art. 2-ter of the Code.

The Company, therefore, with note of the XX, retransmitted on the XX, sent its defense briefs, pursuant to art. 166, paragraph 6, of the Code, in which, after having illustrated the structure and specific characteristics of the same, he declared that:

- "the AOUP staff who, in the last two years, due to the pandemic, have seen a significant turnover among all roles and profiles as well as, in the last period, a substantial number of suspended from the service (both health and administrative ) for refusal to be vaccinated, is made up of hospital employees (extraction at XX equal to n. XX) and university staff working under the convention regime (extraction at XX equal to no. XX). Added to these are all natural persons who, for various reasons, carry out their activities, even temporarily, within the various structures of the Hospital - University of Padua (internal outpatient specialists, holders of freelance positions, scholarships of study, occasional collaborations, co.co.co, work contract, visitors, trainees, extra-network frequencies, volunteers)";
- “out of 19 addresses (…) only 7 are recognizable, while the other twelve are not immediately attributable to the account holder. Furthermore, the serious underlying clinical motivation, common to all those concerned, as well as their extreme interest in accessing any therapy that can bring benefit to their health conditions, could explain how no one has so far complained of a disservice, albeit due to an error ";
- "undoubtedly the violation was culpable, caused, as better indicated below, only by the distraction of the operator not usually involved in this activity. The perpetrator of the violation has certainly not benefited for herself or for others from the violation itself and, as was verified on 24/02 u.s. from the Director of the UOC Cardiac Surgery, there are currently no complaints and/or

reports received from the interested parties following the notification to the Authority";

- "on the 20th day, the Director of the UOC Cardiac Surgery (Privacy Delegate) sent a single @mail to all interested parties, with the text "...We inform you that by mere mistake, completely involuntary, the email addresses of the recipients of the communication have been indicated in clear instead of bcc (in hidden mode). We apologize for the incident and kindly ask you to cancel the email previously sent with unencrypted addresses and not to use these email addresses, as it is illegal";

- "the AOUP with a note signed by the General Manager, as part of a process of continuous information and awareness of the staff, has adopted the following measures:

Company regulations for the use of IT tools, e-mail and the Internet (resolution n.XX ...);

extensive communication, to all personnel, regarding compliance with the provisions contained in the aforementioned Regulation (…);

Training course (Nov/Dec. XX), also aimed at further illustrating the aforementioned Regulation with particular reference to the use of company email and mobile devices, held by the DPO, and addressed to the UOC/UOSD Directors, coordinators and to secretariats;

Circular sent, to all personnel, dated XX on the subject: invitation to respect the use of IT tools as per the Company Regulations adopted with DDG n. XX (…);

sending, on the XX date, to all Personnel, a further circular with the subject "New recommendation on compliance with the correct methods of use of IT tools, as per the Company Regulations adopted with DDG XX";

sending, on the XX date, a further communication to all Personnel on the subject: «Respect for the correct methods of using e-mail accounts»";

- "in view of the violation which occurred and was the subject of notification to the Authority, the Data Controller deemed it necessary to send, again to all Staff, on the XX date, a further and more specific communication containing "operating indications relating to sending emails to other than the addressee and disclaimer»";

- "The Padua University Hospital Company, aware not only of the regulatory obligation but also and above all of the importance that training on the subject of Personal Data Protection plays in order to increase operators' awareness of the risks associated with data processing, plans annually with resolution of the General Manager the training to be provided to the Personnel working in the Company. In the last two years, training has taken place, for the well-known reasons related to the COVID 19

pandemic, via FAD (allowing, among other things, to reach as many people as possible in a short time) or via meet. Initially, the training consisted of a compulsory basic course (…) to introduce the principles, fulfilments and responsibilities dictated by the new legislation (still in progress) and, then, more specific and always compulsory (…) also with the help of the DPO, aimed at illustrating the documentation produced by the Data Controller regarding the Protection of Personal Data. For the XX, training aimed at specific sectors is being planned";

- "also, on the 20th date, the DPO, in attendance, held a specific course in which the topic of technologies was further dealt with, aimed at operators of the company Information Systems UOS on the subject: "IT Security and Data Protection in the Hospital – University of Padua". The course was attended by n. 12 people including those who supervise the management of emails within the UOS";

- "the Company hereby declares its willingness to cooperate with this Authority for the adoption of any further measures to be put in place to remedy the violation and prevent, if possible, the recurrence of similar circumstances in the future (...) . The Company is also available to cooperate with the Authority to mitigate the possible negative effects deriving from the violation, where it de facto deems their existence";

- "by mere mistake, unencrypted e-mails were sent to the interested parties (some sent to addresses from which it seems impossible to derive the recipient's name and surname), which meant that every patient became aware that other patients in the same health situation as you (waiting for a heart transplant) were potentially enrolled in the NIHP 2019 Multicenter study. In fact, the e-mail requested possible participation in this project with the return of the documentation (forms to be filled in and signed for subscription to the study) attached to the same email";

- "the procedure subject to the violation is to be considered absolutely temporary, adopted by the Company in the midst of the pandemic to prevent patients from accessing the hospital. In fact, the Procedure usually provides for the delivery of documentation to patients by hand";

- "the COVID-19 pandemic has negatively affected these fundamental aspects:

1. the person who (…) usually deals with the specific matter was absent (…); the activity was, therefore, necessarily taken over by a colleague, as an unusual and additional task for her with respect to her own competences;

2. the consideration that must be had in the pandemic phase, especially for the most fragile patients, has forced doctors to send the text of the documentation relating to the study via @mail to save them access to the hospital environment and an

interview in person;

3. Recrudescence of the pandemic;

4. Absence of Personnel due to illness, for various reasons, at XX: total no. 322

5. Suspension of Personnel, to the XX, for failing to comply with the vaccination obligation: total no. 201".

The statements made were confirmed by sending copious documentation.

On the 20th date, the hearing requested by the Company was held. In this circumstance, what had already been stated in the defense briefs was substantially reiterated, specifying that:

- "the Company has made a strong commitment to personnel training, as documented in Annex 31 of the corporate communication; furthermore, at the end of the 20th century it carried out a training program specifically aimed at UOC Directors and Coordinators of health professions, specifically aimed at gaining knowledge of the corporate privacy policies on the protection of personal data; in addition, a training course will soon begin for all newly hired personnel and a further training activity extended to all personnel in service relating to the use of telematic tools in communicating with the patient; both training activities were planned in agreement with the company DPO";
- "The Company also underlines that the accident can be attributed to the replacement of the operator normally assigned to this activity, absent from the service, whose duties have therefore been assigned, for reasons of urgency, to an operator not normally assigned to this function (….)";
- "in the specific case, communication via e-mail was necessary, since the recipients of the same are fragile patients and, therefore, certainly, it is inappropriate to convene them in person; in this regard, it should be noted that, compared to the 19 recipients of the message, only 7 were in some way identifiable by their e-mail address, the other addresses being made up of nicknames that cannot be traced back to a personal data";
- "finally, we underline the Company's commitment to implementing all the technologically available measures to guarantee the security of communications to protect the confidentiality of the data of the interested parties".

The Company therefore asked to proceed with the closure of the administrative procedure and, alternatively, the application of a fine as small as possible or a warning provision.

3. Outcome of the preliminary investigation

Having taken note of what was represented and documented by the Company during the proceeding with the violation

notification deeds, with the related defense briefs and during the hearing, it is noted that:

"personal data" means "any information relating to an identified or identifiable natural person ("data subject")" and "health data" means "personal data relating to the physical or mental health of a natural person, including the performance of health care, which reveal information relating to your state of health" (Article 4, paragraph 1, nos. 1 and 15 of the Regulation). The latter data deserve greater protection since the context of their processing could create significant risks for fundamental rights and freedoms (Cons. n. 51 of the Regulation);

with particular reference to the case in question, 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 (Article 9 of the Regulation and Article 84 of the Code in conjunction with Article 22, paragraph 11, Legislative Decree No. 101 of 10 August 2018);

the data controller is, in any case, required to respect 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, through appropriate 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).

4. Conclusions.

In the light of the assessments referred to above, taking into account the statements made by the Company during the investigation and considering that, unless the fact constitutes a more serious offence, 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" □ the elements provided by the data controller in the defense briefs referred to above, although worthy of consideration, do not allow the findings to be resolved notified by the Office with the act of initiation of the procedure of the XX, since none of the cases provided for by art. 11 of the Guarantor's regulation n. 1/2019.

In particular, the arguments put forward by the Company are not suitable for accepting the request for archiving. In fact, in consideration of the definition of personal data referred to above, e-mail addresses can be traced back to the notion of personal data (see Provv.ti of the Guarantor of 25 June 2002, web doc. n. 29864 and 24 June 2003, doc. . web no. 1132562, which can be consulted at www.gpdp.it). In particular, it should be noted that even e-mail addresses without references to the name and surname or in any case to other directly identifying information of the interested parties constitute personal data,

therefore subject to the application of the specific regulation. Furthermore, the circumstance that, from the context of the communication, it could be deduced that the recipients of the e-mail, sent by the Cardiac Surgery Unit, were patients awaiting a heart transplant - who were requested to participate in a specific clinical study by returning the documentation (forms to be completed and signed for participation in the study) attached to the same email - implies that the treatment in question, subject of the notification of violation, concerned health data, as they concern information relating to health care services, which reveal information on the state of health (Article 4, paragraph 1, no. 15 of the Regulation).

Therefore, the sending of the aforementioned communication by means of a single e-mail message addressed to a multiple number of recipients, whose addresses have been entered unencrypted in the carbon copy (cc) field, has, in fact, without justified reason and in the absence of legal prerequisite, mutually revealed to the addressees of the same communication, the state of health of the other patients.

For these reasons, the preliminary assessments of the Office are confirmed and the illegality of the processing of personal data carried out by the Company is noted, for having communicated personal data and data relating to the health of the interested parties (to whom the email addresses pertain), recipients of the communication aimed to acquire informed consent for any participation in a specific clinical study, in violation of the basic principles set out in articles 5, par. 1, lit. f), and 9 of the Regulation.

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

In this context, considering, in any case, that the conduct has exhausted its effects and considering that the Company has declared that it has asked the recipients of the email, to cancel and not to use the email addresses of the other patients and to having adopted further measures deemed necessary to avert future similar events, the prerequisites for the adoption of prescriptive or inhibitory measures pursuant to art. 58, par. 2, of the Regulation.

4. 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. f), and 9 of the Regulation, caused by the conduct put in place by the Company, is subject to the application of the administrative fine pursuant to art. 83, par. 5, 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 College [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, for the case in question, it is noted that:

the Authority became aware of the event following the personal data breach notification made by the data controller and no complaints or reports were received to the Guarantor on what happened (Article 83, paragraph 2, letters h) and k) of the Regulation );

the personal data affected by the violation fall into the particular category of information relating to health (Article 83, paragraph 2, letter g) of the Regulation);

19 data subjects are involved (Article 83, paragraph 2, letter a) of the Regulation);

in relation to the subjective element, no intentional attitude was shown on the part of the data controller, as the violation occurred by mistake when entering the recipients in the specific field of the email by an employee not assigned to this activity, who , for organizational reasons, was called to replace a colleague (Article 83, paragraph 2, letters b) and k) of the Regulation);

the Company has taken charge of the problem by indicating measures aimed at mitigating the damage suffered by the interested parties and reducing the repeatability of the same events that occurred (Article 83, paragraph 2, letter c) of the Regulation);

the controller has demonstrated a high degree of cooperation with the Authority in order to remedy the violations and mitigate their possible negative effects (Article 83, paragraph 2, letter f) of the Regulation);

the fact occurred as part of a temporary procedure, adopted as an initiative undertaken by the Company during the pandemic period, aimed at avoiding, for the delivery of documentation, the summoning in the presence of fragile patients, recipients of

the email, inappropriate due to health risks caused by the Covid-19 pandemic emergency (Article 83, paragraph 2, letter k) 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, of the Regulation, to the extent of 5,000.00 (five thousand) euros for the violation of articles 5, par. 1, lit. 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, also in consideration of the type of personal data subject to unlawful processing.

Finally, it should be noted that the conditions pursuant to art. 17 of the Guarantor's regulation n. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Authority.

ALL THIS CONSIDERING THE GUARANTOR

declares the illegality of the processing of personal data carried out by the Padua University Hospital, for the violation of the articles 5, par. 1, lit. f) and 9 of the Regulation, in the terms referred to in the justification.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the Padua University Hospital Company, with registered office in Via Giustiniani, 2 - 35128 Padua, Tax Code: 00349040287, in the person of its legal representative pro-tempore, to pay the sum of 5,000.00 (five thousand) euros 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, an amount equal to half of the fine imposed.

ENJOYS

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 Euro 5,000.00 (five 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 entire publication of this provision on the website of the Guarantor and

believes that the conditions set forth in 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.

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 bring a judicial 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 January 2023

PRESIDENT

Station

THE SPEAKER

Zest

THE SECRETARY GENERAL

Matthew