[doc. web n. 9779057]

Order injunction against Società Ospedale San Raffaele s.r.l. - April 28, 2022

Record of measures

n. 164 of 22 April 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by 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 national law 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 the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46 / EC (hereinafter the "Code");

GIVEN the legislative decree 10 August 2018, n. 101 on "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 individuals with regard to the processing of personal data, as well as the free circulation of such data and repealing Directive 95/46 / EC ";

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

GIVEN the documentation in the deeds;

HAVING REGARD to the observations made by the Secretary General pursuant to art. 15 of the Guarantor Regulation n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, Doc. web n. 1098801;

Speaker Dr. Agostino Ghiglia;

WHEREAS

1. Violations of personal data

The San Raffaele Hospital s.r.l. (hereinafter "Hospital") notified the Authority of two personal data violations, pursuant to art. 33 of the Regulation, dated XX and XX, concerning, respectively:

a) entering the email addresses of the recipients of a newsletter addressed to patients of the Neurology Operating Unit, in the field called "carbon copy" (CC) in place of the "blind carbon copy" (CCN) field.

In relation to this event, the Hospital announced that:

"Of the 499 email addresses, 321 are names referring to patients, 46 names referring to family members / caregivers and 132 non-names";

as a measure taken to ensure data security, an indication was given to send communications relating to mailing lists, by entering the addresses of recipients in "blind copy" (CCN). In this sense, other initiatives have been adopted: “further and specific training course to make the person responsible for the violation better aware, even though the same occurred due to an accidental act attributable to human error / material error”; "Assessment by the personnel management (of) any disciplinary sanctions against the subject and / or the hierarchical superior"; "Apology emails to interested parties"; "Further training activity (...) by type of authorized subjects"; “Policy and procedure review / improvement action”.

b) the insertion of the email addresses of the recipients of a newsletter addressed to patients of the Transplant and Metabolic-Bariatric Surgery Unit, in the field in the field called "carbon copy" (C.C.) instead of the "blind carbon copy" field (C.C.N.) .

With reference to this matter, the Hospital stated that:

- “of the 90 email addresses, 75 are names referring to patients and / or family members / caregivers and 15 are not directly identifying. The information contained in the newsletter was of a purely organizational nature (opening of the new pavilion), indirect traceability to information suitable for revealing a possible state of health of the person concerned is only possible from the professional qualification of the sender ";
- "following an apology e-mail following the incident, many patients expressed solidarity with the responsible operator, thanking her for the work done and attention to them";

- “New and more effective technical-organizational measures will be implemented through the following internal project: - Establishment of a multidisciplinary working group (Health Department, Internal Audit Department, Company Privacy Executive, Information Systems Department) under the supervision of the DPO; an analytical mapping will be carried out of all the company operating units that need to carry out massive communication activities on patients (communication to +1 patient) with identification of the respective process owners; the individuals identified will receive further specific vertical training on the correct use of the business tools necessary for the execution of the activity; documentation will be prepared for easy and quick consultation (leaflets, infographics or booklets) to supplement the company procedures already in place and distributed to the process owners; discussions are underway with the supplier of the company mailing application (Microsoft) to evaluate the technical possibility of introducing forms of control / management of mass communications; the feasibility of setting up an internal service dedicated to "mass communications", equipped with professional sending tools (mailer) and personnel with specific skills will be assessed ".

In both cases, the hospital represented that it became aware of the violations following a report by an interested party involved in the communication.

2. The preliminary activity

The Office, in relation to the cases described above, on the basis of what is represented by the data controller in the respective acts of notification of violation, as well as subsequent assessments, notified the Hospital, pursuant to art. 166, paragraph 5, of the Code, the initiation of two proceedings for the adoption of the measures referred to in art. 58, par. 2, of the Regulations, inviting the aforementioned owner to produce defensive writings or documents to the Guarantor or to ask to be heard by the Authority (Article 166, paragraphs 6 and 7, of the Code; as well as Article 18, paragraph 1, of Law no. . 689 of 11/24/1981). In particular, respectively, with acts no. XX of the XX and n. XX of the XX, it was found that the Hospital made two communications of personal and health data, respectively, of 498 and 90 patients, to as many patients, in the absence of a suitable legal basis and, therefore, in violation of the principles basis of the treatment referred to in art. 5, 6 and 9 of the Regulations and art. 2-ter of the Code.

Following the aforementioned acts of notification of violations, the Hospital sent its defense briefs, pursuant to art. 166, paragraph 6, of the Code. In particular:

a) with reference to the first case described above (see point 1, letter a)), with a note of the XXth, the Hospital, in addition to

what has already been represented in the notification of the violation of personal data pursuant to art . 33 of the Regulation, stated that:

- "the creation of the newsletter affected by the violation is part of the initiatives that OSR health workers have adopted in the onset of the pandemic emergency from Covid-19 as a tool to respond to the needs of patients and caregivers to receive information and clarifications on the activities of the Unit where patients are being treated and therefore being able, in part, to counteract the sudden lack of direct contact with the hospital and its carers. This initiative was therefore not born as a result of a project conceived and structured by the institutional offices of OSR dedicated to communication activities, where automated processes and systems are in use for the massive sending of emails, also through external suppliers, but as concrete and immediate response of healthcare personnel to the patient's need to maintain tangible proximity to their own care facility ";
- “this activity was entrusted to a subject, duly trained in the use of IT resources and the protection of personal data, competent in managing the assignment received. In fact, in addition to having adopted a code of ethics that expressly contemplates the protection (among others) of interests relating to the protection of personal data, it has informed all its staff about the principles of protection and confidentiality of personal data and " correct use of IT resources, both through contractual confidentiality obligations and through precise instructions that are provided to each employee on the correct processing of personal data in the context of their duties, as well as through specific and detailed instructions on the use of resources IT that expressly describe the need to use only the CCN field for sending mass emails ";
- “the present case was configured as an accidental act attributable to human error. In terms of negligence, in light of the particular circumstances in which the event occurred (this is an isolated case and therefore the exception that confirms the rule), we highlight that OSR has put in place security measures suitable to prevent risks for rights and freedoms of the interested parties and, due to the exceptional nature of the error, it could hardly be argued that OSR could actually have implemented an alternative conduct in this sense ";
- "as regards the seriousness of the alleged violation, (...) in the present case, there is no probability of a concrete and effective risk for the rights and freedoms of the natural persons concerned, understood as the probability of the occurrence of reputational damage, financial loss, discrimination or other significant prejudice for the data subjects, since the scope of communication of the data in violation is limited to other patients or caregivers and restricted to only the email address which, in several cases, does not refer to the patient but to his caregiver and, in several others, it consists of a non-nominative

address and therefore not directly attributable to an immediately identifiable natural person ".

- "of the 499 email addresses communicated in clear text, 321 are nominative addresses referring to patients, 46 names referring to caregivers and 132 are non-nominative addresses, therefore 178 addresses are not email addresses of patients under treatment at the same operating unit, since they are individuals third parties (caregivers) or not directly attributable to identifiable natural persons either as patients or as caregivers ";

- "following the accident that occurred, the person responsible for the error attended a further and specific training course on the protection of personal data and received a letter from the Personnel Department recalling the contractual obligations relating to compliance with the confidentiality and data protection. An apology email was sent to the subjects affected by the violation by the Director of the Unit in question, following which no further notifications or complaints were received from the interested parties on the incident that occurred ";

- "the provision of new and further general and vertical training activities aimed at the entire company population, divided by type of persons authorized to process the processing, and that all the policies and procedures relating to the use of IT tools and the protection of personal data are the subject of an extensive review and update project ";

b) In relation to the second event represented above (see point 1, letter b)), with a note of the XX, the Hospital - in addition to reiterating what has already been explained in a note of the XX, in order to the reasons and methods by which the initiative aimed at creating the newsletter affected by the violation was carried out - it highlighted, among other things, that:

- it is considered (...), in the present case, that there is no probability of a concrete and effective risk for the rights and freedoms of the natural persons concerned, understood as the probability of the occurrence of reputational damage, financial losses, discrimination or other significant prejudices for the interested parties, since: the data object of the communication (email addresses) are personal data not belonging to particular categories, it cannot be considered that the generic origin of the communication in question from the "Transplant and Metabolic-Bariatric Surgery" Unit is in degree - in the specific case, and not only potentially - of disclosing information relating to the state of health of the recipients, not being in itself suitable for disclosing in a concrete and current way a specific pathology or a precise health service from which it can be traced - also indirectly - to a specific state of health. Therefore, on this point, the interpretation of the legislation on the protection of personal data carried out by this Authority (...) is contested, where it is concluded that "Therefore, the information subject to the notification also concerns personal data relating to health" since the generic nature of the services and pathologies related to

the "Transplant and Metabolic-Bariatric Surgery" Unit does not allow the direct identification of "health data" understood as personal data relating to the physical or mental health of a natural person, including the provision of health care , which reveal - and not which could reveal - information relating to the state of health (see Article 4, paragraph 1, no. 15 of the Regulation); the scope of communication of the data object of the communication is indistinctly limited to other patients or their caregivers and restricted to the email address which, in several cases, does not refer to the patient but to the caregiver and, in several others, consists of a non-nominative address and therefore not directly attributable to an immediately identifiable natural person ";

- "of the 90 email addresses communicated in clear text, 75 are nominative addresses referring to patients and / or their caregivers, and 15 are non-nominative addresses that cannot be directly linked to either patients or their caregivers";
- "therefore it is in no way possible for the recipients of the newsletter in question to make a concrete - and not merely potential or random - distinction between which email addresses belong to patients (the only interested parties to whom the" data relating to the health ") and which to caregivers (to whom, in any case, only personal data not belonging to particular categories - email addresses - and not data relating to health would refer)";
- "following the accident that occurred, the person responsible for the error was made aware of the protection of personal data and compliance with company procedures aimed at protecting personal data and will attend a further and specific training course on the subject in question . An apology email was sent to the subjects affected by the violation by the Director of the Unit in question, as a result of which no further notifications or complaints were received from the interested parties on the accident that occurred, but rather certificates of solidarity and solidarity were received. estimate towards the operator who made the material error ";
- "An analytical mapping was carried out of all the corporate operating units that need to carry out massive communication activities on patients (communication to +1 patient) with identification of the respective process owners and these subjects will be provided with further vertical, specific training , about the correct use of the company tools necessary for the execution of the activity ";
- "following discussions with the supplier of the company mailing application (Microsoft), a specific Microsoft tool (" Power Automate for desktop ") For the management of mass communications; the personnel belonging to the aforementioned directions will be involved in specific training activities for the use of the tool, including a general part of training on the

protection of personal data and violation of personal data and a specific and technical part on the use of the new tool Microsoft, with practical demonstrations of specific features ";

- "Finally, the following further technical-organizational measures will be put in place: (i) provision of new and further general and vertical training activities aimed at the entire company population, divided by type of subjects authorized to process; (ii) extended project of review and update of all policies and procedures relating to the use of IT tools and the protection of personal data ".

For the reasons set out above, in both cases, the Hospital asked the Authority to qualify the reprimand within the limits of slight or very slight negligence, so as to provide for the application of non-pecuniary corrective sanctions and, only in the alternative, if it deems to provide for the application of pecuniary sanctions, to commensurate this sanction in the minimum terms.

Taking into account that the violations subject to notification pursuant to art. 33 of the Regulations concern the same data controller and similar cases, the Office has ordered the meeting of the two investigative proceedings, pursuant to art. 10, paragraph 4 of the regulation of the Guarantor n. 1/2019, and communicated this circumstance to the data controller with the aforementioned note of the XX.

3. Outcome of the preliminary investigation

Having acknowledged what is represented and documented by the Hospital during the two investigative proceedings referred to in point 1, lett. a) and b), first with the acts of notification of violation and, subsequently, with the related defense briefs, it is noted that:

"personal data" means "any information relating to 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 performance of health care, which reveal information relating to your state of health "(Article 4, par. 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. No. 51 of the Regulation);

the Regulation provides that the processing of personal data is lawful only if and to the extent that one of the conditions provided for by art. 6 of the Regulations;

with particular reference to the issues raised, the 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

Article 84 of the Code in conjunction with 'art.22, paragraph 11, legislative decree 10th August 2018, n.101);

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 ensure 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).

4. Conclusions.

In light of the aforementioned assessments, taking into account the statements made by the data controller during the investigation and considering 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 deeds 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" notified by the Office with the aforementioned acts of initiation of the proceedings, however, none of the cases provided for by art. 11 of the regulation of the Guarantor n. 1/2019.

In particular, the arguments put forward by the Company are not suitable for accepting the archiving requests formulated in the defense briefs. In fact, in light of the definition of personal data referred to above, the e-mail addresses, as already highlighted in the notes of the twentieth and twentieth centuries, are attributable to the notion of personal data (see Provisions of the Guarantor of 25 June 2002, doc. web n. 29864 and 24 June 2003, web doc. 1132562, available at www.gpdp.it). Therefore, even if part 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 the subject of personal data protection. Furthermore, the circumstance that from the context of the communications it could be inferred that the recipients of the same were users, in one case, of the Neurology Unit and, in the other, of the Transplant and Metabolic-Bariatric Surgery Unit and, therefore, patients in care at the aforementioned Units, implies that the treatments, with respect to which the data breach notifications were made to the Guarantor, concerned information relating to health, as it concerns information relating to health care services, which reveal information on state of health (art. 4, par. 1, n. 15 of the Regulations). Therefore, the sending of communications by means of a single e-mail message addressed to a multiple number of recipients, whose addresses have been entered in the carbon copy field (cc), has, in fact, without justified reason and in the absence of a legal basis , mutually revealed, to the recipients of the communications, the state of health of the other patients.

For these reasons, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by the Hospital is noted, for having communicated to third parties the personal data of the interested parties to whom the email addresses refer, recipients of the aforementioned communications, of which to this proceeding, as well as data relating to health, in violation of the basic principles referred to in Articles 5, lett. f), and 9 of the Regulations.

The violation of the aforementioned provisions makes it applicable, pursuant to art. 58, par. 2, lett. i), 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.

In this context, considering, in any case, that the conduct has exhausted its effects and considering that the Hospital has declared that it has adopted further measures deemed necessary to prevent future similar events, the conditions for the adoption of measures do not exist, of a prescriptive or inhibitory nature, pursuant to 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).

Violations of Articles 5, par. 1, lett. f), and 9 of the Regulations, caused by the conduct put in place by the Hospital, are subject to the application of a pecuniary administrative sanction pursuant to art. 83, par. 5, of the Regulation.

Consider that 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, of the Regulation in relation to which, for the cases in question, it is noted that:

the Authority has become aware of the events following the notifications of violation of personal data made by the owner and no complaints or reports have been received to the Guarantor on the incident (Article 83, paragraph 2, letters h) and k) of the Regulation) ;

the data processing carried out by the hospital also concerned data suitable for detecting information on the health of a few hundred data subjects (Article 83, paragraph 2, letters a) and g) of the Regulation);

from the point of view of the subjective element, no intentional attitude emerges on the part of the data controller, since the violations occurred by mistake in the phase of entering the recipients in the specific email field (Article 83, paragraph 2, letter b) of the Regulation);

the Hospital has taken charge of the problem by introducing measures aimed at reducing the replicability of the same events that occurred (Article 83, paragraph 2, letter c) of the Regulations);

the owner 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 facts occurred as part of the initiatives taken by the Hospital to respond to the needs of patients and caregivers to receive information and clarifications on the activities of the Unit where patients are being treated, in an attempt to counteract the sudden lack of contact direct with the hospital structure determined by the pandemic emergency from Covid-19 (Article 83, paragraph 2, letter k) of the Regulation).

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, of the Regulations, to the extent of € 70,000.00 (seventy thousand) for the violation of Articles 5, par. 1, lett. f) and 9 of the Regulations, 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 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 the regulation of the Guarantor n. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Authority.

WHEREAS, THE GUARANTOR

declares the unlawfulness of the processing of personal data carried out by the San Raffaele Hospital Company, for the violation of Articles 5, par. 1, lett. f) and 9 of the Regulations, within 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 San Raffaele Hospital Society s.r.l, with registered office in Via Olgettina 60 - 20132 Milan, P.I. and Tax Code: 07636600962, in the person of the pro-tempore legal representative, to pay the sum of € 70,000.00 (seventy 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, an amount equal to half of the sanction imposed.

INJUNCES

to the aforementioned San Raffaele Hospital s.r.l., in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 70,000.00 (seventy 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 lodge 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 applicant resides abroad.

Rome, April 28, 2022

THE VICE-PRESIDENT

Cerrina Feroni

THE RAPPORTEUR

Ghiglia

THE SECRETARY GENERAL

Mattei