

Injunction order against the Provincial Health Service Agency of Trento - April 21, 2021

Record of measures

n. 155 of 21 April 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 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 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 n. 1/2019");

GIVEN 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 and the investigation activity

The Authority received a report and two complaints regarding the processing of personal data carried out by the Provincial

Health Services Agency of Trento (hereinafter the Company) through the company health dossier (called "Hospital Information System" - SIO). In particular, repeated accesses to the dossier were reported by health personnel who, although authorized for treatment, were not involved in the process of treating the subjects to whom the health files referred.

1.1 Complaints regarding repeated access to the company health dossier of two subjects linked by emotional ties

In February and July 2020, the Authority received two complaints, respectively by Ms XX and comrade Mr. XX, regarding repeated accesses to their corporate health dossiers carried out - between 2017 and 2019 - by personnel of the diagnostic radiology department of the S. Lorenzo Hospital in Borgo Valsugana (belonging to the aforementioned Company) which, according to what they reported claimants, appear to be similar and connected.

In relation to the aforementioned complaints, the Office, in arranging the meeting of the proceedings, requested information from the Company (notes of 24.6.2020, prot. No. 23217 and of 15.7.2020, prot. No. 26426), which feedback provided with note dated 13 August 2020 (prot. no. 117264). In this deed, the Company acknowledged that Dr. XX, XX, and represented that: regarding the consultation of Ms XX's health file, dr. XX, with report dated 11 March 2020, stated that "the undersigned and Mrs. XX have been in a sentimental relationship since the end of January 2016, during which I have been authorized on several occasions - always only verbally, as usually happens in similar situations - to consult their health data, in order to book specialist visits and examinations. If I remember correctly, I have also issued one or more commissions. The fact that even in recent times he has made access is related to a state of affective concern for his state of health. Obviously I have never disclosed or communicated to third parties the health data of Mrs. XX ". In this regard, the Company specified that: "Dr. XX, although it does not appear that the system was in charge of the person concerned, accessed Mrs. XX's data because she used, under her own responsibility, some of the reasons provided for in the IIS for health protection purposes and listed below: "Anamnestic check at the request of the doctor or for diagnostic completion "," Clinical assistance needs before a specialist visit "and" Diagnostic needs ";

regarding the consultation of the health dossier of Mr. XX, Dr. XX stated that "that the accesses to the SIO related to Mr. XX, for which justification is sought, occurred by mistake ";

"In relation to the possible profiles of disciplinary relevance that emerged in the context of the investigation conducted on the above cases, the Corporate Disciplinary Procedures Office (UPD) was invested, which activated against Dr. XX a disciplinary procedure, still in progress ";

"With reference to the same persons involved in these complaints, a criminal proceeding is underway, (...) with reference to which" the APSS provided the documentation relating to the accesses made by Dr. XX to the health file of Mrs. XX and Mr. XX".

In relation to the results of the aforementioned investigation, the Office, with deed no. 33864 of 15 September 2020, notified the Provincial Health Services Agency of Trento, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in Article 58, paragraph 2, of the Regulations, inviting the aforementioned holder 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, of the law n. 689 of 24/11/1981).

In particular, the Office, in the aforementioned deed, in recalling the obligations of the Company, as data controller, to allow access to the health record only to personnel who for various reasons intervene in the treatment process of the interested party, represented that Dr. XX, a doctor working at the aforementioned Company, accessed the health files of Mrs. XX and her current partner Mr. XX in the absence of a suitable legal basis and without their knowledge and, therefore, in violation of the basic principles of the treatment referred to in art. 5 and 9 of the Regulations.

With a note dated October 15, 2020 (prot. No. 150669), the Company sent its defense briefs, in which, in particular, it was represented that:

the disciplinary procedure against Dr. XX "has expired due to the termination of the employment relationship between APSS and the Medical Director in question, pursuant to art. 55 bis, paragraph 9, Legislative Decree 165/2001, without prejudice to the civil and criminal liability of the same doctor and the right to recourse to the Administration in the event of any claims for compensation";

"As soon as it became aware of the accesses, the Company has undertaken various initiatives (...) aimed at improving the technical and organizational measures relating to the methods of access to the DSE and which provide for changes to the Hospital Information System (SIO), according to the indications contained in the Guidelines on the electronic health dossier of this Ill.ma Authority of 4 June 2015";

"In the context of the SIO, at the time of the facts covered by these complaints, access to the reports could take place not only through the presence of an open contact (access to the emergency room, hospitalization, consultation and outpatient visit) also through the 'SIO - Report History' interface by entering one of the reasons encoded in the system";

"With regard to the actions to improve the technical and organizational measures undertaken by the APSS, with effect from 15 October 2020, a first measure was introduced which provides for the disabling of the "SIO - Historical Reports" interface for most of the operators. It follows that, due to this change, access to the reports can now take place for health protection purposes only by qualified operators who have an open contact with the patient (access to the emergency room, hospitalization, service consultation and outpatient visit) and which therefore intervene in various capacities in the patient care process. The "SIO - Report History" function therefore remains active exclusively for a limited number of specifically authorized operators as they are employed in specific sectors of activity that necessarily require access to users' health records even in the absence of direct contact with them (...). It should be noted that the implementation of these new rules will be completed by 1 December 2020 ";

"The Company, also following the reports received, intends to implement a procedure for carrying out random checks, in compliance with the legislation for the protection of workers, aimed at verifying that the behavior of the operators in the use of the IIS complies with the regulations on the protection of personal data and corporate procedures. On 13 October 2020, the General Manager also sent all staff a communication via e-mail to make them aware of the behaviors to be adopted in order to respect the confidentiality of patients, recalling the company rules and procedures on data protection. personal data available on the company intranet in the "Privacy section";

"With regard to the willful or negligent nature of the violation (...), if from the point of view of the subjective profile of the author of the access it can be configured as willful misconduct or negligence, any intentional infringement of the confidentiality of the interested parties must be absolutely excluded on the part of the APSS."

1.2. reporting on access to the health file by medical personnel not involved in the treatment path of the person concerned

In August 2020, the Authority received a report from Ms XX, with reference to the accesses made to the health dossier of the Provincial Health Services Agency of Trento called "Hospital Information System" (SIO). According to what was reported, in April 2020 Ms XX received 27 notifications of access to her health data through the SIO application carried out by a doctor on duty at an APSS hospital in Trento. With reference to the aforementioned accesses, the reporting party produced a note from the aforementioned Company in which the "healthcare professional admitted his responsibility, while charging it with an innocent error for homonymy" (note of 11 June 2020, prot. No. 85274).

In relation to the aforementioned report, the Office requested information from the Company (note of 16 September 2020, prot.

No. 34070), which provided feedback with a note of 16 October 2020 (prot. No. 935332). In this deed, the Company represented that:

"Mrs. XX became aware of the accesses autonomously because, in recent years, the Company had activated a service consisting of sending an automatic notification message (alert) that alerts her in real time of any access to your data through the SIO application as a security, control and transparency measure ";

"On 3 May 2020 he communicated to the lady the results of the checks carried out by the Technology Department, as well as what was declared by the doctor concerned with reference to the accesses made that would have occurred by mistake";

"The doctor concerned had accessed Ms. XX's data on a single occasion and not through multiple independent accesses: within this single access he then viewed a plurality of reports";

"At the time of the facts, access to the reports could take place not only through the presence of an open contact (access to the emergency room, hospitalization, consultation and outpatient visit) also through the " SIO - Historical Reports "interface. Through this interface, the operator could search the client's documentation by name, surname and date of birth, by entering at least three letters of the name and three letters of the client's surname. Once the elements for the search were entered (example: part of the client's name and surname), the system proposed a list of clients who met the criteria entered by the operator. The results of the research appeared on a screen distributed over various lines, one for each client, to facilitate reading. Each line contained the following information: surname, name, sex, date of birth, tax code, municipality of residence and municipality of birth of the assisted person ";

"By selecting a client from the list of search results, an assisted detail sheet with complete personal data was opened first. Subsequently, through the button "SIO - History pag. 3 Reports "the system proposed a new screen that required the selection of a reason from a predefined list (with compilation of the mandatory notes field) for access to the reports. Once the reason was selected, only at that point did a screen appear containing the list of reports that can be consulted based on the consent expressed by the client. In order to view the contents of each report, it is necessary to select it and open it to see it in its entirety in the format originally produced. The search for a client, as well as the selection of a preview report and the opening are recorded in the application logs ";

"Having said that, with reference to cases of homonymy (same name and surname) or homocody (cases in which name, surname, date of birth and place of birth are the same and generate the same tax code for more than one client) it is specified

as follows. The cases of homonymy / homocody appear in the assisted search results screen marked by lines with a red background, differentiating from the other lines with a white / yellow background. In the event that a client belonging to one of the two types described above (homonymy / homocody) is selected, the system offers a screen containing only the names concerned, and asks the operator to confirm his choice ";

"In order to prevent repetition of episodes such as the one reported, improvement actions have been planned to the HIS aimed at restricting access and therefore visibility to the patients' reports, which will also lead to a reduction in the risk of incorrect access by operators to health documents relating to patients characterized by homonymy or homocody. It should be noted that the implementation of these new rules will be completed by 1 December 2020 ";

"The Company, also following the reports received, has planned the implementation of a procedure for carrying out random checks, in compliance with the legislation on the protection of workers, aimed at verifying that the behavior of the operators complies with the regulations regarding the protection of personal data and company procedures ";

"On 13 October 2020, the General Manager also sent all staff a communication via e-mail to make them aware of the behaviors to be adopted in order to respect the confidentiality of patients, recalling the company rules and procedures regarding the protection of personal data available on the company intranet in the "Privacy section".

In relation to the results of the aforementioned investigation, the Office, with deed no. 39697 of 23 October 2020, notified the Provincial Health Services Agency of Trento, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in Article 58, paragraph 2, of the Regulations, inviting the aforementioned holder 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, of the law n. 689 of 24/11/1981).

In particular, the Office, in the aforementioned deed, in recalling the obligations of the Company, as data controller, to allow access to the health record only to personnel who for various reasons intervene in the treatment process of the interested party, as well as what is indicated in the notification of violation pursuant to art. 166, paragraph 5, of the Code already sent to the aforementioned Company as part of the investigation described in the previous paragraph, represented that the configuration of the health record carried out by the Company allowed a doctor operating at the same to consult, "through a single access to the system ", numerous health documents of the reporting woman without being involved in the treatment path of the same concerned and, therefore, in violation of the basic principles of the treatment referred to in Articles 5, par. 1, lett. a)

and f) and 9 of the Regulations.

With a note dated 20.11.2020 (prot. N. 175952) the Company asked to be heard by the Authority and sent its defense briefs, in which, in particular, the start of the "adaptation process "" On the methods of accessing the historical reports through the Hospital Information System (SIO) "which had already been illustrated in the defense briefs sent as part of the preliminary procedure described in the previous paragraph, to which reference should be made.

In particular, the Company reiterated that "on 15 October 2020 it proceeded with the disabling of the" SIO - Historical Reports "interface and specified that" an "Emergency Urgency" button was activated to allow qualified health professionals to they operate in some specific company contexts to access the patient's historical reports to manage urgent emergency situations (eg urgent opinion of the cardiologist requested in the operating room, diagnostic classification of the patient arriving in the emergency room, etc.) ".

It was also highlighted that the Company also intervened "on departmental applications (eg radiology, laboratory, gastroenterology, etc.) so that when the operator has in charge a patient for the execution of a service (eg. CT, resonance), can access the reports repository of the HIS for the purposes of diagnostic classification as the HIS itself "recognizes" the open contact on the departmental application ".

With specific reference to the emergency context for the spread of Covid-19, the Company has shown that, compared to what it had previously indicated in the defense briefs relating to the investigation indicated in the previous paragraph, the complex of interventions "on the IIS has nevertheless generated difficulties of an operational nature reported by various health professionals, who complained about the difficulty of accessing the reports repository even in the presence of open contact with the client. Considering that, in the current emergency context, the patient often cannot physically go to the hospital, they also reported the need to have access to the patient's clinical history even in the absence of an active outpatient visit, for example to respond to a urgent request for an opinion from the general practitioner or a request for consultation from the patient himself ".

It was therefore represented that "in the face of these repeated reports from healthcare professionals, the Company deemed it appropriate in the immediate future, in order to avoid an impact on the health of patients and taking into account the period of high stress for the healthcare facilities involved in dealing with the Covid-19 emergency, restore the previous mode of visibility on the Historical reports, planning a more gradual introduction of the above measures. APSS has therefore implemented the

following initiatives:

1. preparation of a document with operating instructions (Annex 1) for personnel with the new rules for accessing the reports repository through the SIO;
2. before sending to the staff the document referred to in point 1 was subjected to a sample of doctors in order to collect any observations or critical issues;
3. sending informative emails to staff (on 3, 4 and 6 November 2020 - Annex 2) on the start of a stress test on 6 November and simultaneous transmission of the instructions for page 3 access the historical reports through the HIS;
4. performance of the stress test on 6 November 2020 ".

The Company also highlighted that "following the stress test, the operators again complained of difficulties in managing the operational change introduced at this historical moment, due to the workload and the emotional tension to which they are subjected to manage of the serious health emergency in progress. The Company therefore decided immediately, in order not to aggravate the situation of health workers already tried by the emergency situation and in conditions of work stress, to proceed with some risk mitigating measures, as described below, reserving the full implementation of the measures planned at the end of the state of emergency, and more precisely:

1. keep the SIO-historical report button active for assistance purposes in the absence of open contact with the patient (hospitalization, outpatient visit, PS access, consultancy, direct access) by conditioning access to the reports by the operator to the following rules, to guarantee the protection of the confidentiality of the clients (these actions are to be carried out cumulatively for each access carried out):

- selection of one of the reasons provided for in the system, which follow the case history of the assistance activities to be guaranteed to the patient (e.g. anamnestic check at the request of the doctor or for diagnostic completion, clinical assistance needs before a specialist visit, examination of examinations at the request of the patient, assessment pre and post hospitalization, clinical assistance needs for territorial services);

- mandatory compilation of a notes field in which to specify the legitimacy to carry out the activity in relation to the individual case (e.g. urgent opinion requested in the operating room, diagnostic classification of the patient arriving in the ER, request from the patient or the caregiver of date X etc.);

- activation of a special flag in the system with which at the time of access the operator is made aware that the use of the SIO -

report history button is allowed only for the protection of the patient's health, declaring that access is relevant it is necessary for the assistance activity to be provided and to be aware of the consequences in terms of disciplinary, civil and criminal liability in the event of a false declaration and therefore in the event of improper access; (this measure which is expected to be introduced from 1 December 2020)

2. keep the SIO-historical report button active for purposes of public interest pursuant to art. 2 sexies of the Privacy Code (e.g. requests for judicial authorities, requests for medical records, epidemiological activities) only for a limited and defined number of operators specifically authorized in relation to the role covered, and according to the rules and guarantees provided for in point 1;

3. immediate activation, subject to prior information (...) to the staff, of random checks on accesses carried out via the SIO report historical button;

4. continue with carrying out periodic stress tests in order to encourage a gradual and less invasive introduction, given the current context, of the adjustment measures described above;

5. plan a training and information activity for staff to facilitate the introduction of the new rules, to be implemented at the end of the pandemic; Once the state of emergency has been overcome, APSS will complete the adjustment in question.

In relation to the Company's request made in the aforementioned note of 20.11.2020, on 27 January 2021, at the Office of the Guarantor, pursuant to Articles 166, paragraphs 6 and 7, of the Code 18, paragraph 1, by law no. 689 of 11/24/1981 the hearing of the aforementioned Company took place, during which the same reiterated what had already been represented, specifying in particular that:

"The worsening of the pandemic emergency in progress, as indicated in the aforementioned memoirs, led to the suspension of the implementation of the actions described above. (...). In the current emergency context, it was considered appropriate not to fully complete the changes envisaged on the procedures for accessing the HIS for operators, in order to speed up their intervention on the System. The emergency would then have made it difficult to carry out the necessary training activity for the operators. In this regard, it should be noted that the Company is the only one operating on the territory of the Province, with a catchment area of approximately 540,000 inhabitants ";

"The completion of the measures indicated in the defensive briefs on the health dossier will take place within approximately three months of the end of the current state of emergency. In the meantime, specific training campaigns for health personnel

will be launched, as well as sample checks on access to the file will be implemented ";

"The functionalities of the SIO not yet implemented concern:

limitation of the possibility of allowing access to the file in the absence of the physical presence of the interested party (historically referable to about 4% of accesses) for specific reasons only to certain categories of operators (eg emergency departments). The implementation of this measure has been suspended due to the difficulties in making the necessary organizational changes and the related appropriate information campaigns to users in the emergency context; adoption of an IT solution that can be used by the corporate control bodies that highlights the accesses that may present elements of anomaly, up to the provision of automatic alert systems ";

"The provision of diversified access to information systems for corporate administrative bodies, so that they can access, within the limits of the powers provided for by law, a more complete information base than that present in the company health dossier";

"As of December 1, 2020, the following measures have already been implemented:

- reduction of the time bands of access by the health worker (limitation of the temporal depth of access);
- strong reduction of the possibility of access to the IH of patients in charge of the operator who logs in, but who are not physically present in the company at that time, through a limitation of the cases allowed and providing that the operator must declare the cause of access and must acknowledge the relative responsibility of such declarations;
- the implementation of the aforementioned measures made it possible to carry out more precise checks on the accesses made by the operators ".

With a subsequent note dated February 10, 2021 (prot. No. 26617), the Company sent the "Plan for adjusting the procedures for accessing the historical reports through the Hospital Information System (SIO)" which describes in detail the phases of the process implementation of the technical and organizational measures to be adopted with reference to the company health record.

2. Outcome of the preliminary investigation.

With reference to the treatments covered by the aforementioned report and the aforementioned complaints, the Guarantor has adopted the "Guidelines on the health dossier - 4 June 2015" (Provision of 4.6.2015, published in Official Gazette 164 of 17 July 2015, available on [www .gpdp.it](http://www.gpdp.it) doc web n.4084632), which, like the other provisions of the Authority, continue to apply

even after the full application of the Regulation, as they are compatible with it (Article 22, paragraph 4, Legislative Decree no. 101/2018).

In the aforementioned Guidelines, the Guarantor, in order to avoid the risk of unauthorized access to information processed through the health dossier or communication to third parties of health data by authorized persons, specifically asked the owner of the treatment to pay particular attention to the identification of the authorization profiles and the training of the authorized subjects, access to the dossier must be limited only to health personnel who intervene in the patient care process and technical methods of authentication to the dossier must be adopted that reflect the cases of access to this tool specific to each health facility. To this end, in the aforementioned Guidelines, the Guarantor has indicated to the data controllers to carry out a monitoring of the hypotheses in which the related health personnel may need to consult the health file, for the purpose of treating the interested party and, based on this recognition, identify the different access authorization profiles.

Access to the dossier must therefore be limited only to healthcare personnel who intervene over time in the patient care process. This means that access must only be allowed to personnel who in various capacities intervene in the treatment process. Access to the dossier must then be limited to the time in which the treatment process is articulated, without prejudice to the possibility of accessing the dossier again if this is necessary regarding the type of medical treatment to be provided to the person concerned.

Having said that, having taken note of what is represented by the Company in the defense briefs relating to the proceedings indicated in the previous points 1.1 and 1.2, it is noted that:

1. the accesses subject to the complaints referred to in paragraph 1.1. they were not carried out by a doctor in order to provide treatment services to the interested parties, but for other reasons with reference to which criminal proceedings are underway;
2. the accesses subject to the report referred to in paragraph 1.2. they were carried out by a doctor due to a repeated homonymy error in the patient identification phase;
3. the aforementioned complaints and the aforementioned report made it possible to highlight that the measures adopted by the Company, with reference to the treatments carried out through the company health dossier, did not allow to avoid the possibility that the qualified health personnel had access to the clinical documentation of patients not treated by them, resulting in the unlawful processing of personal data concerning the interested parties, in violation of articles 5 par. 1, lett. a) and f) and 9 of the Regulations;

4. in particular, the Company has adopted technical and organizational measures that have proved to be not fully adequate in order to ensure adequate security and integrity of personal data, including protection from unauthorized processing as established by art. 5, par. 1, lett. f), of the Regulations;

5. the Company has implemented measures aimed at limiting access to patients' health records to only health personnel who treat them only after having ascertained the episodes subject to the aforementioned complaints and the aforementioned report, identifying logical-IT solutions which are based, in fact, on the indications already provided by the Guarantor in the aforementioned 2015 Guidelines (see paragraph 6 of the aforementioned Guidelines) and reaffirmed in the measures adopted by the Authority on the matter since 2013 and published on the Guarantor's website (see provisions of 10.1.2013 - doc. web n. 2284708, of 3.7.2014 - doc. web n. 3325808, of 23.10.2014 - doc. web n. 3570631, of 18.12.2014 - doc. web n. 3725976 , of 22.10.2015 -doc web n. 4449114 and of 22.6.2016 - doc. web n. 5410033, most recently provision of 23 January 2020, doc. web n. The preventive adoption of these measures, also in light of the principles of data protection from design (privacy by design) and by default (privacy by default) contemplated in art. 25 of the Regulations, could have prevented (or limited) the aforementioned unauthorized accesses to the company health files subject to the aforementioned complaints and the aforementioned report;

6. the implementation path of the technical organizational measures on the procedures for accessing the HIS for health professionals has been only partially completed, due to the need to ensure, in the emergency context in progress, that the intervention of the operators on the aforementioned system is as quickly as possible, as well as to complete the training activity regarding the new access procedures, the implementation of which has become more complex in the current emergency situation;

7. with the measures already adopted by the Company following the aforementioned preliminary activities, the time bands of access to the HIS by health professionals have been reduced, the cases of access to the HIS limited with reference to the dossiers of patients not physically present in the Company and controls on access by operators implemented;

8. The Company stated that the completion of the aforementioned measures will take place within approximately three months of the end of the current state of emergency; in particular, within the aforementioned term the cases of access to the HIS will be further limited with reference to the dossiers of patients not physically present in the Company, IT solutions adopted that highlight the accesses that may present elements of anomaly, and a method of access to the systems will be identified

diversified information for corporate administrative bodies.

3. 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 information 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" by the Office with the acts of initiation of proceedings for the adoption of corrective and sanctioning measures, however, 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 Provincial Health Services Agency of Trento with reference to the aforementioned proceedings initiated following the complaints and reporting described in points 1.1 and 1.2 of this provision, within the terms of which in motivation, in particular, for having processed personal data in violation of articles 5, par. 1, lett. a) and f), and 9 of the Regulations.

In this context, considering, in any case, that in both the procedures described above the conduct has exhausted its effects, given that the Company has already implemented organizational technical measures on the procedures for accessing the company health file for health professionals, as well as declared that the completion of the aforementioned measures will take place within three months of the end of the state of emergency for Covid-19, in consideration of which it is not possible to proceed with the completion of the same in a shorter time and that with regard to the facts covered by the complaints cited in the paragraphs 1.1 of this provision a criminal proceeding has been initiated against the author of the access, 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. l and 83 of the Regulation; art. 166, paragraph 7, of the Code).

The violation of articles 5, par. 2, lett. a) and f), and 9 of the Regulations, caused by the omissive conduct of the Provincial Health Services Agency of Trento, is subject to the application of a pecuniary administrative sanction pursuant to art. 83, paragraph 5, of the Regulation.

In consideration of the fact that the aforementioned proceedings concern the same owner, processing of similar personal data, which occurred in a short period of time and that the Company in the defense briefs relating to the procedure referred to in

paragraph 1.2 has also provided elements concerning the procedure described in par. 1.1 (see note dated 20.11.2020, prot. .

It should be considered 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. 85, par. 2, of the Regulation in relation to which for both proceedings it is noted that:

- the Authority became aware of the event following two complaints and a report (Article 83, paragraph 2, letter h) of the Regulations);
- in the case of the proceeding initiated following the report (par.1.2), the interested party became aware of access (made by mistake several times but on a single occasion) to her health file by virtue of the alert system adopted by the Company (Article 83, paragraph 2, letter a) of the Regulations);
- in the case of the proceeding initiated following the two complaints (paragraph 1.1), the accesses were made intentionally by an authorized person within a period of three years (Article 83, paragraph 2, letter a) of the Regulation);
- although access to the health dossier of the complainants and the whistleblower was carried out, in both procedures, by personnel authorized by the Company intentionally - in the case of the procedure referred to in par. 1.1 - and by mistake - in the case described in par. 1.2- this was possible because the measures put in place by the Company with reference to the data processing suitable for detecting health information carried out through the company health dossier were not fully proportionate in order to guarantee adequate security and integrity of personal data and to prevent unauthorized access (Article 83, paragraph 2, letters a), d) and g) of the Regulations);
- the Company has implemented measures aimed at limiting access to patients' health records only to health personnel who treat them only after having ascertained the episodes covered by the aforementioned complaints and reports, identifying

logical-IT solutions based on , in fact, on the indications already provided by the Guarantor in the aforementioned 2015 Guidelines (Article 83, paragraph 2, letters a), b) and d) of the Regulation);

- the events were immediately taken over by the Company, followed by the identification of corrective and resolving solutions that were almost entirely adopted also in conjunction with the emergency context in which the data controller operates (Article 83, paragraph 2, letter c) of the Regulation);

- the Company immediately demonstrated a high degree of cooperation even if strongly committed to the management of the Covid-19 pandemic situation (Article 83, paragraph 2, letter f) 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, lett. a) of the Regulations, for the violation of articles 5, par. 1, lett. a) and f) and 9 of the Regulation to the extent:

- 40,000 (forty thousand) for the procedure described in paragraph 1.1; And
- 10,000 (ten thousand) for the procedure described in paragraph 1.2;

which administrative pecuniary sanctions withheld, 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 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, in both the procedures described, by the Provincial Health Service Agency of Trento, for the violation of art. 5, par. 1, lett. a) and f) and 9 of the Regulations in the terms set out in the motivation.

In this regard, pursuant to art. 157 of the Code, the Company to communicate within three months of the end of the state of emergency approved by the Council of Ministers the completion of the technical organizational measures indicated in the "Plan for the adaptation of the procedures for accessing the historical reports through the Hospital Information System (SIO) "sent

with a note dated 10 February 2021 (prot. No. 26617); any non-response may result in the application of the pecuniary administrative sanction provided for by art. 83, paragraph 5, of the Regulation.

ORDER

pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, to the Provincial Health Services Agency of Trento, based in Trento, Tax Code / VAT number no. 01429410226, to pay:

the sum of € 40,000 (forty thousand) as a pecuniary administrative sanction for the violations detected with reference to the complaints presented by Ms XX and Mr. XX indicated in this provision;

the sum of € 10,000 (ten thousand) as a pecuniary administrative sanction for the violations detected with reference to the report presented by Ms XX indicated in this provision;

according to the methods indicated in the annex, within 30 days from the notification of motivation; 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 sanctions imposed.

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 sums of € 40,000 (forty thousand) and € 10,000 (ten thousand) according to the methods indicated in the annex, within 30 days of notification of this provision, under penalty of 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, April 21, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei