SEE ALSO NEWSLETTER OF 26 JULY 2022

[doc. web n. 9790365]

Injunction order against the Friuli Centrale University Health Authority - 26 May 2022 *

Record of measures

n. 201 of May 26, 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, Professor Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, members and dr. Claudio Filippi, Deputy Secretary General;

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

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

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

Professor Ginevra Cerrina Feroni will be the speaker;

WHEREAS

1. The violation of personal data and the investigation activity

The Authority received two notifications of violation and a complaint regarding the processing of personal data carried out by the Central Friuli University Health Authority (hereinafter ASUFC) through the company health dossier (called "Report Viewer"). 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 Notifications of violation regarding access to an employee's company health record by company medical staff.

The ASUFC with a note of the XX (prot. N. XX), notified a violation of personal data representing that "on XX, two employees of the Company had access to the medical report viewer - health file of a patient who is at the time an employee himself, in the absence of a valid legal basis, becoming aware of data concerning the state of health of the same ", as well as having" become aware of the violation following the reporting of the interested party "and that in this regard" it was disciplinary proceedings started against employees who made improper access and a complaint was presented to the Public Prosecutor's Office at the Court of Udine ".

In relation to the aforementioned notification of violation, the Office requested information with the notes of the XX (prot. N. XX), of the XX (prot. N. XX) and of the XX (prot. N. XX), with reference to which the ASUFC responded with the notes of the XX, XX and XX signed by the person responsible for the protection of personal data, in which it was, in particular, represented that:

- "the DSE works with the Report Viewer application, provided by INSIEL SPA. Access to the Viewer is reserved for healthcare personnel" and "allows healthcare staff to access data relating to the healthcare services of patients who are being treated at the structure";
- access to the dossier is allowed under the following conditions: "a) if the patient is under treatment, that is, he is hospitalized in a ward, or is in the emergency room, or a booked outpatient visit is in progress, his data are accessible to health personnel; b) if the patient is not under treatment, access to data through the Report Viewer is subject to the issuance of a declaration of responsibility by the health care worker, who must make a choice between the four alternative conditions ";

"If the patient is not hospitalized in the facility from which access to the Report Viewer is accessed, access to the data is subject to the issuance of a declaration of responsibility by the healthcare professional, who must make a choice between four alternative conditions of access authorization. The lack of the option is "blocking" and the session cannot continue ";

the declaration of responsibility is as follows: "" I declare under my responsibility that I have the right to continue viewing the

data for activities of:

- Prevention / diagnosis / treatment / rehabilitation on patients in charge but not registered in the planned computerized paths - Critical review for analysis and possible improvement of treatment paths;

- Harvest / transplant process

- Health Department - support for organizational processes and regulatory compliance "";

- "The declarations are recorded, like all the accesses made through the Report Viewer, in order to allow the subsequent verification of the legitimacy of such accesses, and this in the case of requests for access by the interested party pursuant to art. 15 of the GDPR, or where doubts arise in this regard ".

- "The Report Viewer is accessible only by authorized doctors and nurses under the following conditions:

a) if the patient is present in the Company, that is, he is hospitalized in a ward, or is in the emergency room, or a booked outpatient visit is in progress;

b) if the patient is not present, the circumstance that the patient intervenes in the treatment process is the subject of a specific declaration by the staff who intend to access the data, to be transmitted through the Report Viewer application by selecting one of the four alternative conditions already mentioned in the previous note of the XX.

The present case falls within the case cited above sub b), since the interested party was not present at the time of accessing the data shown in the notification of violation of the XX ";

with reference to the secure communication protocol, "we inform you that the new Report Viewer, for which the relative and gradual implementation is already underway, will support the" https "protocol with effect from XX, at the end of the necessary adaptation activities of the entire dedicated infrastructure. This implementation may in any case suffer delays also in relation to events that cannot be foreseen today or to a different prioritization of the needs defined by the competent Regional Central Management "(Insiel's note of the XX, prot. XX).

In relation to the results of the aforementioned investigation, the Office, with deed no. XX of the XX, notified the ASUFC, 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, 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, the Office highlighted that the configuration of the health dossier carried out by ASUFC identifies a single access profile, thus allowing all health personnel to access the health files of any patient who is present in the Company at that time. regardless of the fact that the same is actually being treated by the person making the access, without any time limitation.

The Office then noted that the failure to identify different access profiles makes it clear that not only has been taken into account the fact that only the staff who are currently treating the patient can access the file, but also that not all healthcare personnel can be authorized to carry out the same personal data processing activities through the dossier.

It was also noted that, as required by the aforementioned Guidelines, a system for detecting any anomalies that may constitute illegal processing, or the use of anomaly indicators (so-called alerts) aimed at identifying anomalous behavior or risk relating to the operations performed by the persons authorized to process the processing (e.g. number of accesses performed, type or time frame of the same), useful for guiding subsequent audit interventions.

In the aforementioned deed it was also highlighted that ASUFC uses the "http" (hypertext transfer protocol) network protocol for the processing in question which, in addition to not guaranteeing the confidentiality and integrity of the data exchanged between the user's browser and the server hosting the application, does not allow users to verify the authenticity of the server they are talking to.

In spite of this, the violation of the basic principles of processing pursuant to art. 5, par. 1, lett. a) and f), of the Regulations and subsequent articles 9, 25 and 32. The violation of the aforementioned provisions makes the administrative sanction provided for by art. 83, par. 4, lett. a) and par. 5, lett. a) of the Regulations.

With a note of the XX (prot. N. XX) the ASUFC sent defensive writings and asked to be heard, representing, in particular, that the fact to be notified concerned "Mrs. XX, formerly an employee of the same Company at the UO First Aid of Latisana, as a result of unauthorized access - through the Report Viewer application - by a doctor, Mr. XX, and a nurse, Mrs. XX, both working in the same ward as the person concerned ". the accesses would have occurred "all on 24/09/2020, respectively from 2.30 to 2.33 (access of Mrs. XX), and from 3.22 to 3.28 (Mr. XX). In both cases, since Ms. XX was not present in the health facility at the time of accessing the data, both the nurse and the doctor - in order to access the data - declared under their own responsibility that they had the right to continue with the visualization of the data for the activity of "Prevention / diagnosis / treatment / rehabilitation on a patient assigned but not registered in the computerized paths provided" ". The ASUFC in this act contested what the Office represented in the note of the XX, considering that "the health services provided by the ASUFC are

quantitatively and qualitatively extremely numerous, heterogeneous and interdisciplinary, so that it does not appear possible to establish a priori rigid temporal rules on accessibility to data for treatment purposes, precisely because the patient care process can be characterized by the provision of very different services, rendered in different times and places and by professionals belonging to different disciplines ".

It was also specified that "with regard to the accessibility of data by the staff of the Health Department of the ASUFC, also subject to dispute in the notification of the violation of the XX, it should be noted that this question, in addition to having no relevance with the present case clearly falls within the notion of treatment for the purpose of care pursuant to the aforementioned art. 9.1.h) of the RGPD ".

With regard to the communication protocol used by the Company, the same stated that "It is not clear, in fact, how the adoption of the" HTTPS "protocol could have prevented or avoided the violation of Mrs A.R's data (...). However, it has been indicated that, in a period of time that appears reasonable, the new report viewer will support the "HTTPS" protocol ".

During the aforementioned investigation, the ASUFC, with a note of the XX (prot. No. XX), notified a further violation of personal data relating to a case similar to that previously notified described in the previous paragraph.

In particular, in the aforementioned communication, the AUFC declared that it had verified, following a patient report, that "in a period of time between 2018 and 2020, some employees of the Company had access to the report viewer - health dossier of a patient who is at the same time an employee, in the absence of a valid legal basis, becoming aware of data concerning the state of health of the same ". In this case, as stated in the documents, "all the operators have declared that they have the right to continue consulting the documentation for" prevention / diagnosis / treatment / rehabilitation on patients in care but not registered in the computerized paths provided ".

In the aforementioned communication, the ASUFC then specified "that disciplinary proceedings have been initiated against employees who have made improper access and a complaint will be presented to the Public Prosecutor's Office at the Court of Udine" and that it intends to proceed with a " greater awareness of staff on the correct use of IT tools and the consequences deriving from their improper use; periodic and systematic checks aimed at verifying the correct use of company tools ".

In view of this, the Office with a note of the XX (prot. No. XX) brought together the investigative proceedings relating to the notifications of violation of the XX and XX and notified the ASUFC, 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, par. 2, of the Regulation, reiterating what has

already been contested with the note of the XX and inviting the aforementioned holder 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 art. 18, paragraph 1, of the law n. 689 of 11/24/1981).

With a note of the XX (prot. N. XX) the ASUFC, in asking to be heard, sent defensive writings, where it reiterated what has already been represented in the documents, specifying that "the data breach of Mrs. XX, an employee of the same Company at the Rehabilitation Pneumology department of the Gervasutta hospital "occurred" as a result of unauthorized access - through the Report Viewer application - by three doctors and a nurse, all working in the same department as the person concerned. (...) unauthorized access would be eleven, which occurred between 22/10/2018 and 04/12/2020. The four employees, to whom the accesses are attributable, were consulted and all excluded having made such accesses personally, having no professional reasons or personal interests that justify such conduct. They hypothesize that the accesses to the data were carried out by unknown persons who, having access to shared computers, would have entered a work session left open for reasons of urgency. The ASUFC therefore initiated the disciplinary procedure and at the same time filed a complaint with the judicial authorities for the hypothesis of a crime pursuant to art. 615-ter of the Criminal Code ".

With a subsequent note of the XX (prot. No. XX) the ASUFC renounced the hearing it had previously requested.

1.2. Complaints regarding access to an employee's company health record by company medical staff

In the month of XX, the Authority received a complaint from Ms XX who complained about "multiple accesses" to the information system that manages the ASUFC health file "not related to therapeutic and / or clinical needs" by professionals operating in the rehabilitation pneumology department of the Gervasutta hospital belonging to this company, where, among other things, the complainant works ".

Following the Office's request for information (note del XX, prot.n.XX), the ASUFC represented that the aforementioned complaint refers to the violation of personal data notified by the Company on the XXth, on which the Office had the sanctioning procedure has already begun (note of the XX, prot. no. XX).

1.3. The involvement of the Friuli Venezia Giulia Region and subsequent preliminary stages

As part of the investigation launched following the aforementioned violation notifications and similar investigations initiated against other health companies of the Friuli Venezia Giulia Region regarding the processing of personal data carried out through the health file, it emerged that all health companies belonging the regional health service (SSR) have established the

company health dossier using the application called "viewer reports" made available by Insiel S.p.A ..

According to what was stated in the investigative documents, the configuration of the corporate health dossier would have been carried out according to standard rules defined by Insiel under the coordination of the aforementioned Region, with a view to uniformity and homogeneity at the information level of the Regional Health Service. In particular, the configuration of the health file made available by Insiel actually allowed health personnel to access the file relating to any patient who was physically present in the health company at that time and, declaring the existence of a plurality of preordained cases, also to those of patients not present in the Healthcare Company.

In spite of this, the Office - with a note of the XX (prot.no.XX) - highlighted the critical aspects identified in the current configuration of the health dossiers, mainly related to the authorization profiles, to the Friuli Venezia Giulia Region and to the health authorities involved. provided for access to the health dossier and alert systems. In this note, the Office proposed a meeting with the aforementioned Bodies, in order to deepen the characteristics of the information system made available by Insiel to the regional health companies ("report viewer") through which they created the company health file , as well as the margin of autonomy recognized to healthcare companies in the implementation of the measures deemed necessary by them, as data controllers, in order to make the processing compliant with the regulations on the protection of personal data.

Following the aforementioned meeting, which took place remotely on the 20th, the aforementioned Region sent a note in which the "adaptive interventions of the" Report Viewer "system were summarized, in order to eliminate or at least minimize the critical issues identified" (note of the XX, prot. n. XX).

In the aforementioned note, the "current situation" was described, that is the "general rules, valid for the whole Region:

• Display of documents on the basis of the consents given by the interested party, with the exception of: o documents obscured on a regulatory basis (HIV, genetics, pregnancy loss, etc.) o or documents obscured promptly at the request of the citizen (by the doctor , during the diagnosis and treatment process, or upon request, even later, by the interested party);

• In the absence of an administrative take-over (for hospitalization, access to the emergency room, or for the provision of an outpatient or consultancy service), the data are accessible only on explicit self-declaration with motivation (for example, in the case of a chronic patient who contact the facility by phone and need an opinion for the continuation of home care). "

The Region also specified that "at the expense of each owner, it is possible, through its system administrators, to intervene on the system configurations to:

• Enable operators to access the system, assigning them specific roles, among those agreed between the bodies operating in the regional health system;

• Identify the operating units for which to completely exclude the documents generated from visibility (for example, the reports of the competent doctor);

• Define, for each operating unit, the type of document to be displayed (report, discharge letter, transfer letter, emergency room report, ...) and its status (final, digitally signed, ...);

• Obscure single documents, by the medical editor ".

With reference to the access system to the "report viewer", the Region specified that "there are no administrative roles, as they are not relevant to the purposes of the system".

The aforementioned note also briefly described the "planned adjustments". In particular, with reference to the visibility of documents accessible through the aforementioned "report viewer" it was stated that:

• "Access without self-declaration can be restricted only to operating units for which an administrative acceptance has been opened. For outpatient episodes or requests for advice, the opening is valid for the solar day of opening; for first aid, until discharge; for hospitalizations, up to discharge / transfer.

• If it is necessary to access the dossier of patients not present from an administrative point of view (for example, to view reports received following hospital discharge), it will be necessary to fill in the self-declaration, giving reasons for the access. In all cases where the patient is not administratively present in the facility that accesses the viewer, self-declaration is required ".

With regard to the timing of the implementation of the aforementioned adjustments, it was stated that they can be made "in two distinct phases:

• First phase (more restrictive): all operators access with self-declaration, regardless of whether the patient is administratively present in the specific operating unit. The solution can be implemented within 10 working days of the request;

• Fully operational: allows the facility that has the patient present for administrative acceptance (ward, clinic, PS, RSA, ...) to access documents without self-declaration. For all other structures, self-declaration is mandatory. Gradual implementation of the new viewer on the various calling systems over a period of 6 months ".

With regard to the "Alert tools" it was reported that "in the space of three months, additional data warehouse functions will be released, which can be consulted and customized by each owner. It will be possible to cross-reference the data of access to

the system, of the self-declarations compiled, of the patient's employee status. The dashboards that will be made available will allow you to monitor the self-declaration cases, the frequency of consultation, etc. In addition to a set of views and summaries that will be made available to all companies, each owner, through his system administrators, will be able to independently define extracts and summaries, to refine the monitoring and detection of any anomalies ".

Having acknowledged what was declared in the aforementioned note, the Office, in order to define the investigative proceedings initiated against the regional health authorities, including the ASUFC, with a note of the XX (prot. No. XX), asked the aforementioned Region information on the current state of implementation of the "adjustments" described above; the methods of access to the report viewer provided for in the event that the interested party is present for administrative acceptance in an operating unit other than the one making the access; the margin of autonomy recognized to healthcare companies in requesting, as data controllers, the company Insiel, already designated by the same companies responsible for the treatment, the modification or personalization of the aforementioned adaptation measures, with particular regard to the configurations relating to the access to the health file; the cases that may be the subject of the aforementioned "self-declaration", with particular reference to those, hitherto permitted, relating to the "health management (support to organizational processes and regulatory compliance)" and to the "critical review, for analysis and possible improvement of care pathways ", indicated in the documents in the deeds; the type of information recorded in the log files relating to accesses and operations performed; the measures to be taken to ensure that access to the health record using the "report viewer" application, when carried out by outpatient clinics outside the companies, can only be carried out with reference to the files of the interested parties being treated at the aforementioned outpatient clinics.

In response to the aforementioned request for information, the Friuli Venezia Giulia Region replied with a note of the XX (prot. No. XX) declaring, in particular, that "a process of verification and analysis will be activated on the systems already supplied to health companies, in order to evaluate their possible application in the field of external prisons / clinics, in compliance with the legislation relating to the processing of personal data ".

Attached to the reply, the Region provided a note from Insiel of the XX (prot.no.XX) in which the Company represented that: "The adjustment foreseen in the first phase can be activated, at the regional level and after consultation with the data controllers, within 15 days of receiving the request":

• Completion of the "fully operational phase" by June 2022. The implementation of the fully operational phase envisages that

the administrative taking over of the patient takes place at the level of the individual operating unit. The activity includes:

• a phase of analysis and planning of developments and the assessment of the organizational impact on company operators (by February / March 2022);

• the adaptation of the clinical-health management systems that invoke the Report Viewer and that indicate the administrative management of the patient for the specific operating unit; the adjustments will have to allow the current operation until the completion of the releases (by May 2022);

• the adaptation of the Report viewer which receives the information on taking charge at the operating unit level for which a specific administrative acceptance of the patient concerned is open and only in this context allows access to the patient's dossier without expressing a self-declaration (by the first half of June 2022);

• the activation of the adjustments on the health agencies, with simultaneous training of the operators on the new methods of use (by June 2022).

• The release of the monitoring dashboards indicated in the “Alert tools” section is confirmed by March 2022;

• In the case of an operating unit other than that in which the interested party is present for administrative acceptance, access to the Report Viewer can only take place after the operator's self-declaration, with an indication of the reason;

• The current selectable items in the self-declaration form are shown below:

Prevention / diagnosis / treatment / rehabilitation on patients in charge but not registered in the planned computerized paths (for example pre / post hospitalization or pre / post outpatient service, consultancy between colleagues of the same company).

Critical review for analysis and possible improvement of the care pathways (for example audits, RCA, sentinel events, etc. as required by law).

Harvesting / transplantation process (for example organ harvesting from a corpse donor to guarantee the best treatment process).

Health Department: support for organizational processes and regulatory compliance (for example, mortuary police activities, diagnosis, cause of death, absence of crime or infectious disease). There is also a notes field where the operator can enter a free text. It is possible to modify / extend / delete the items in the list according to specific needs or different organizational methods that could be put in place.

• particular implementation requests that modify the general functioning are evaluated at the regional level and proposed as an

evolution for all companies

• The audit tables record the data of the operator who accessed the Report Viewer, his / her structure and, in the case of self-declaration, the specific reason indicated will also be recorded. Furthermore, for each patient, their details are recorded and if the display was limited to the list of their documents, or if the operator has also viewed the details of the specific document ".

2. Outcome of the preliminary investigation.

With reference to the treatments covered by the aforementioned violation notifications and the aforementioned complaint, 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 for consultation on 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, d .lgs n. 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 holder 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 be allowed only to personnel who in various ways 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.

With the provision of 10 January 2013 (web doc. No. 2284708), the Authority had already intervened regarding the processing of data carried out through the information system for archiving and reporting the health services provided by the health

structures of the Friuli Venezia Giulia Region, called " G2 "attributable to the instrument of the health dossier. In this provision, the Guarantor had identified specific critical issues relating to the information and consent of the interested parties, access to the health file and the right of obscuration such as to detect the unlawfulness of the treatment carried out by a regional health company and prescribing itself the necessary measures to make the processing lawful.

In this provision, the Authority had also prescribed to health companies and scientific hospitalization and care institutes in the Region that used the same information system to make the processing of personal data carried out through the company health files compliant with the prescriptions dictated. to the aforementioned company within the same terms.

With specific reference to the aspects of the processing covered by this provision, or to the need for access to the file to be allowed only to the personnel who actually cares for the data subject, in the aforementioned provision the Guarantor had deemed it necessary to prescribe specific measures to be implemented -Even possibly making use of the technical support provided by Insiel- which allow only health professionals who are currently treating the patient (who has already given informed consent to the creation of the dossier) to access his health dossier for the time in which the treatment path is articulated.

Following the adoption of the aforementioned provision in 2013, the Guarantor adopted the guidelines on the health dossier (2015) also applicable to the health dossier held by the ASUFC. With the full application of the Regulation, the Company was also required to adapt this information tool to the principles of data protection from the design stage and by default referred to in art. 25 of the Regulation.

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, it is noted that:

1. The configuration of the health dossier prepared by Insiel and currently used by the ASUFC allows health personnel to access this information tool relating to any patient who is physically present in the Company at that time regardless of their actual involvement in the care path of the same and, declaring the existence of a plurality of preordained cases, also to patients not present in the Company. According to what is stated in the aforementioned note of the XX, in fact, "access to patient data" is always allowed to health personnel working at this company "when this is present in the company, hospitalized in a ward or in the emergency room or during a visit booked outpatient ". This approach does not ensure that only healthcare personnel who are actually treating the patient can access the company file, given the fact that not all healthcare professionals intervene in the process of treating all patients hospitalized in the Company's wards (including that of emergency and urgency)

or who benefit from an outpatient health service. As the cases subject to violation demonstrate, in fact, the current configuration of the file has made it possible for health personnel working at the Company to have access without restrictions to the health file of colleagues or interested parties who were not - at the time of access - treated by them, in violation of the basic principles of the treatment referred to in Articles 5, par. 1, lett. a) and f) and 9 of the Regulation, as well as the principles of data protection from design (privacy by design) and by default (privacy by default) contemplated in art. 25 of the Regulation;

2. The configuration of the health dossier prepared by Insiel and currently used by the ASUFC - also in light of the adjustments proposed by the Friuli Venezia Giulia Region - allows access to the health dossier also by the staff of the Health Department for activities of "support to organizational processes and regulatory compliance ", for" Critical review for analysis and possible improvement of care pathways (for example audits, RCA, sentinel events, etc. as required by law) "and for" Collection / transplant process (for example collection activities from organ to corpse donor to guarantee the best treatment process) ". In this regard, it should be noted that, given what has already been represented by the Authority in the aforementioned Guidelines and in other provisions (see provision of 21 April 2021, n- 155), according to which, taking into account the right of blackout exercisable by the interested party data accessible through the health dossier and therefore the possible incompleteness of this information tool, the owner must identify, in relation to the various functions to which the staff is assigned, technical organizational solutions that allow the administrative bodies of the health management to access, within the limits of attributions provided for by law, to a more complete information base than that present in the company health dossier;

3. The configuration of the health record prepared by Insiel and currently used by the ASUFC also does not respect the principle according to which access to the file must be limited to the time in which the treatment process is divided, without prejudice to the possibility of accessing the file again. dossier if this is necessary regarding the type of medical treatment to be provided to the interested party. On this point, in the aforementioned defensive briefs, the Company represented that "the health services provided by the ASUFC are quantitatively and qualitatively extremely numerous, heterogeneous and interdisciplinary, so that it does not appear possible to establish a priori rigid temporal rules on accessibility to data for care, precisely because the patient care process can be characterized by the provision of very different services, rendered in different times and places and by professionals belonging to different disciplines ". These elements do not appear to be sufficient to derogate from the necessary temporal identification of the period of validity of the access profile to the dossier,

given that what is reported does not appear to be a condition that exempts the owner from the application of the general principles of treatment or a unique characteristic of this Company. ;

4. The configuration of the health dossier prepared by Insiel and currently used by the ASUFC does not include a system for detecting any anomalies that may result in illicit treatments, or the use of anomaly indicators (so-called alerts) aimed at identifying anomalous behavior or risk relating to the operations performed by the persons authorized to process the processing (e.g. number of accesses performed, type or time frame of the same), useful for orienting subsequent audits in violation of the principles of integrity and confidentiality of personal data (articles 5, par 1, letter f) and 32 of the Regulation;

5. the ASUFC uses the "http" (hypertext transfer protocol) network protocol for the processing in question which, in addition to not guaranteeing the confidentiality and integrity of the data exchanged between the user's browser and the server hosting the application, does not allow users to verify the authenticity of the server they are talking to. Taking into account the nature, object and purpose of the processing, as well as the risks affecting the data and the possible "cloning" of the system in question for the acquisition of data transmitted for illegal purposes, the solution adopted by the Company cannot be considered a suitable technical measure to guarantee an adequate level of security for the risks presented by the processing, which involves the transmission of data, including health-related data, over a public communications network. Failure to use cryptographic techniques to transport data therefore constitutes a violation of art. 5, par. 1, lett. f), and art. 32 of the Regulation, which, however, in par. 1, lett. a), expressly identifies data encryption as one of the possible security measures suitable for guaranteeing a level of security appropriate to the risk (on this point, see also recital no. 83 of the Regulation in the part in which it provides that "the owner of the processing […] should assess the risks inherent in the processing and implement measures to limit those risks, such as encryption "). In fact, the ASUFC should have put in place, right from the design of its service, adequate technical and organizational measures, aimed at effectively implementing the principles of data protection, including the principle of "integrity and confidentiality", providing to adopt a secure network protocol, such as the "https" protocol (hypertext transfer protocol over secure socket layer), within the system in question. According to what has been declared in the documents, the system in question will use the secure communication protocol https: “with effect from April 2022, at the end of the necessary adaptation activities of the entire dedicated infrastructure. This implementation may in any case suffer delays also in relation to events that cannot be foreseen today or to a different prioritization of the needs defined by the competent Regional Central Management "(Insiel's note of the XX, prot. XX). As things stand, no assurance has been

provided regarding compliance with this deadline;

6. the aforementioned notifications of violation and the complaint made it possible to highlight that the measures currently adopted by the Company, with reference to the treatments carried out through the company health dossier, did not make it possible to avoid the possibility that the qualified health personnel had access to the clinical documentation of patients not treated by them, resulting in an unlawful processing of personal data concerning the interested parties, in violation of Articles 5 par. 1, lett. a) and f), 9 of the Regulations;

7. the Friuli Venezia Giulia Region has illustrated in the notes in the documents the program of a summary process of adaptation of the information systems used by the regional health authorities and the aforementioned Guidelines according to the findings formulated by the Office with reference to the investigative proceedings in place that indicates a certain adjustment period only for some of the necessary fulfilments. in particular, according to what has been declared, it is expected by:

to. 10/15 days from the Company's request as owner: "First phase (more restrictive): all operators access with self-declaration, regardless of whether the patient is administratively present in the specific operating unit";

b. February / March 2022: "a phase of analysis and planning of developments and the assessment of the organizational impact on company operators";

c. May 2022: "the adaptation of the clinical-health management systems that invoke the Report Viewer and that indicate the administrative responsibility of the patient for the specific operating unit";

d. June 2022: "the adaptation of the Report viewer which incorporates the information on taking charge at the operating unit level for which a specific administrative acceptance of the patient concerned is open and only in this context allows access to the patient's dossier without express a self-declaration ";

And. June 2022: "the activation of the adjustments on the Healthcare Trusts, with simultaneous training of the operators on the new methods of use";

f. March 2022: "the release of the monitoring dashboards indicated in the" Alert tools "section;

g. an undefined term: "a process of verification and analysis will be activated on the systems already provided to health companies, in order to evaluate their possible application in the context of prisons / external clinics, in compliance with the legislation on the processing of personal data ".

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 o circumstances o 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 ASUFC with reference to the aforementioned proceedings initiated following the communications of violation and the complaint, in the terms set out in the motivation, in particular, for having processed personal data in violation of articles 5, par. 1, lett. a) and f), 9, 25 and 32 of the Regulation.

In this context, considering that in both proceedings described above, criminal proceedings were initiated against the author of the access and that the adjustments necessary to overcome the critical issues described above, with the exception of the use of the "http ", Are part of a more general rethinking of the characteristics of the health dossier used by the health authorities of the Friuli Venezia Giulia Region by the same and by the company Insiel S.P.A. it is deemed necessary to order the ASUFC, pursuant to art. 58, par. 2, lett. d), of the Regulation, the following corrective measures:

- adopt, within 15 days from the notification of this provision, a secure network protocol, such as the "https" protocol (hypertext transfer protocol over secure socket layer), as part of the medical report viewer system used for the company health record ;
- adopt the measures indicated in the provision approved by this Authority on the same date also against the Friuli Venezia Giulia Region and Insiel S.P.A. to which reference is made in full.

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

The violation of articles 5, par. 2, lett. a) and f), 9, 25 and 32 of the Regulations, caused by the conduct of the ASUFC, is subject to the application of the pecuniary administrative sanction pursuant to art. 83, paragraphs 4 and 5, of the Regulations.

In consideration of the fact that the aforementioned proceedings concern the same owner, in relation to the processing of similar personal data, which occurred in the same period of time and that the Company in the defensive briefs relating to the aforementioned proceedings has provided the same defensive elements, it is considered appropriate to adopt the respective

administrative sanctions in a single provision (articles 10, paragraph 4, and 19 of the Guarantor Regulation no. 1/2019).

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. 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 notifications of violation and a complaint (Article 83, paragraph 2, letter h) of the Regulations);

- with reference to all the events subject to notification and complaint, the illicit accesses concerned the health file of two patients who were at the same time employees of the Company by health professionals (2 in the case of the notification of the XX and 4 in the case of the notification of the XX and of the complaint received) who were not involved in the treatment process of the same and against which disciplinary proceedings were initiated and a complaint was submitted to the Public Prosecutor's Office of Udine (Article 83, paragraph 2, lett. . a) and b) of the Regulations);

- in the case of violation of 20.1.2020 the accesses occurred on 24.9.2020, while in the case subject to the notification of violation on XX, on which the complaint was also presented, between 2018 and 2020 (11 accesses) (Article 83, paragraph 2, letters a) and b) of the Regulations);

- the aforementioned accesses were possible because the measures currently in place 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 avoid unauthorized access even though the Authority had already intervened in this regard with the aforementioned provision of 10 January 2013 and subsequently with the guidelines of 2015 ((Article 83, paragraph 2, letter d) of the Regulation);

- the evidence shows a limited power of intervention by the Company regarding the adoption of additional measures with respect to those predefined by the Friuli Venezia Giulia Region and by the company Insiel S.P.A. on the information system adopted by the ASUFC as a health dossier (Article 83, paragraph 2, letter g) of the Regulation);

- the request by ASUFC to the Friuli Venezia Giulia Region and Insiel s.p.a. has not been documented in documents. corrective actions to the information system called report viewer in order to make it compliant with the Regulation and the measures indicated by the Guarantor in the aforementioned guidelines of 2015 (Article 83, paragraph 2, letter g) 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:

- 25,000 (twenty-five thousand) for the proceeding initiated following the notification of violation of the XXth; And

- 45,000 (forty-five thousand) for the proceeding initiated following the notification of violation of the XX and the complaint presented by Ms XX;

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 Friuli Centrale University Health Authority, for the violation of art. 5, par. 1, lett. a) and f), 9, 25 and 32 of the Regulation in the terms set out in the motivation.

ORDER

pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, to the Friuli Centrale University

Healthcare Company, Tax Code / VAT number no. 02985660303, to pay:

the sum of Euro 25,000 (twenty five thousand) as a pecuniary administrative sanction for the violations detected with the notification of violation of the XX indicated in this provision;

the sum of € 45,000 (forty-five thousand) as a pecuniary administrative sanction for the violations detected with the notification of violation of the XX and with the complaint presented by Mrs. 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 25,000 (twenty-five thousand) and 45,000 (forty-five thousand) euros 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 from art. 27 of the law n. 689/1981;

• pursuant to art. 58, par. 2, lett. d), of the Regulations, to the Friuli Centrale University Health Authority within the term of 30 days from the notification of this provision, to adopt a secure network protocol, such as the "https" protocol (hypertext transfer protocol over secure socket layer), in scope of the report viewer system used for the company health record.

In this regard, the Company is requested to communicate which initiatives have been undertaken in order to implement the aforementioned provisions in this provision and in any case to provide adequately documented feedback, pursuant to art. 157 of the Code, within 15 days from the expiry of the term indicated above; any non-response may result in the application of the pecuniary administrative sanction provided for by art. 83, paragraph 5, of the Regulation

HAS

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

Pursuant to art. 78 of the Regulation, of art. 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision, it is possible to appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of

communication of the provision itself or within sixty days if the applicant resides abroad.

Rome, May 26, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Cerrina Feroni

THE DEPUTY SECRETARY GENERAL

Philippi

* The provision was challenged