SEE ALSO Newsletter of 28 November 2022

[doc. web no. 9819792]

Injunction order against Local Health Authority Valle d'Aosta - 10 November 2022

Register of measures

no. 371 of 10 November 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

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

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national legal 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 movement of such data and which repeals Directive 95/46/EC (hereinafter the "Code");

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

HAVING REGARD to the documentation in the deeds;

GIVEN the observations made by the Secretary General pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web no.1098801;

Speaker the lawyer Guido Scorza;

WHEREAS

1. The complaint and the preliminary investigation

The Authority received Ms XX's complaint in which she complained of repeated access to her company health dossier by a health worker working at a rehabilitation facility of the local health authority of Valle d'Aosta, where she declared that you have never received health care. The complainant also represented that she had denied consent to the processing of her personal data through the company health dossier.

In relation to what has been reported, for the profiles of competence in the field of personal data protection, the Office requested information from the aforementioned Company with a note dated XX (prot. n. XX), with reference to which the latter replied with the note of the XX in which it was represented, in particular, that:

- "the complainant XX appears to have expressed NO consent to the dossier on 01/30/2019 (...). Until 03/17/2020 (when it was deemed appropriate to temporarily deactivate the dossier rules for the reasons described in the following par. HEALTH DOSSIER SITUATION IN A COVID EMERGENCY, page 5) the will expressed by the patient was respected and therefore the operators involved in the treatment process could only consult the clinical data/documents generated by the respective structures to which they belong (in compliance with the provisions of the Guidelines on health dossiers - 4 June 2015)";
- “following an internal investigation, the truthfulness of what was reported by the complainant emerged. Specifically, from the access logs to the dossier (...) it emerged that Ms. XX (with temporary employment relationship at the writing Company), belonging to the "speech therapist" profile (...), in the period from 03/15/2021 to 06/12/2021 accessed from his workstation at the Consultorio di Saint Pierre, (encoded in the company health information system as "Riab. Terr. ST. PIERRE"), pertaining to the Complex Structure called "Districts 1-2 ”;
- "it can certainly be said that the operator did not view clinical documents relating to the results of the visits she had, having only been able to view a list of episodes already carried out or booked, which only shows the type of service";
- "This type of visualization was made possible, even though the complainant was not being treated at the Saint Pierre Consultory on the dates subject of the report, since, starting from 03/17/2020, due to the Covid emergency, the 'Company has authorized a relaxation of the rules of visibility of the dossier”;
- "TrakCare (an ERP - Enterprise Resource Planning- type application which has as its objective the management of all hospital and outpatient functions)" "on which almost all the data rotates and converges" is in use at the aforementioned Company. In the solution used by the Local Health Authority of Valle d'Aosta, the territorial activities are also managed electronically by TrakCare. In addition to the aforementioned management system, the clinical information system consists of

further vertical solutions (so-called producer systems) which generate clinical documents which, after digital signature, are sent to the X1V1 Repository (intermediate archiving system between the producer systems and the actual of digital preservation), which can also be recalled from TrakCare for consultation of the documents". "At the state of the art it was agreed that TrakCare could assume the role of dossier";

- with "prot. note no. XX" the aforementioned Company asked "the Intersystems company, owner of the TrakCare product, to implement the rules of visibility of the information as per the indications of the Guidelines" of the Guarantor of 2015. The procedure described below was therefore carried out: a) the managed operational flow provides in the first instance, upon recall of any patient registry, the verification of the presence or absence of consent to the creation of the dossier and, in the event that the patient has not yet expressed it, its collection. b) based on the profiling of the operators and on the basis of the context (patient being treated or not, episode with blackout request, etc...), the system applies the necessary filters that define whether or not information is displayed. c) in TrakCare each operator is assigned to a "group/profile". The "group/profile" he belongs to determines what he can "do" and what he can "see". When the privacy filters are active, based on a matrix of rules, TrakCare allows the operator to see and possibly operate only on episodes pertaining to the profile. The expression of consent to the dossier and whether the patient is "under treatment" (i.e. there is an "open/current" episode) for the operator's specialty are also taken into consideration". "Furthermore, to govern possible emergencies or particular cases, a function called "Break The Glass" has been implemented that can be activated only by doctors, which cancels all filters allowing you to view all the information present in the system on condition that you have recorded the reason for the use";

- "Precisely this partial visibility of the "speech therapist" profile prevented the operator who made improper access from being able to consult the reports of the services performed by the complainant even in a situation of deactivation of the dossier rules, allowing him only a view of the lists of episodes booked or made, but without the possibility of entering the individual episodes and viewing the clinical documentation produced";

- "All data display actions (access log) are tracked and can only be extracted by certain authorized operators";

- "From a clinical point of view, the emergency context has forced (and still today obliges) the hospital to merge almost all of the non-COVID wards and to create dedicated COVID wards" "with all the resulting managerial, clinical and organizational consequences" "It was therefore necessary to allow access, according to the needs of the moment, to the health information of TrakCare. In fact, according to the strict rules of the dossier previously in force, the health professionals referred to above,

doctors and other health professionals belonging to different specialist structures and/or disciplines, could not, in fact, have access to the medical records and health data of hospitalized patients in COVID wards (formally assigned to the Pulmonology department) or in multi-specialist non-COVID wards and therefore would not have been able to adequately care for patients";

- "In relation to medical personnel, in the initial phase it was recommended to use the "Break the glass" (...) to make up for the impossibility of viewing the complete data of the current and historical situation of the patients for whom they were not authorized. However, the use of this function entailed a considerable burden in operations (this function must be activated for each individual episode and search with an indication of the reason), so in order to allow adequate usability for the management of the pandemic in progress, with note Prot n.XX of the XX (see Annex XX), the Company Health Director has authorized the disabling of the Health dossier, until the end of the state of emergency";

- "In this regard, we believe it necessary to underline how the easing of the rules on the dossier first found its legal basis in art. 14 of the Legislative Decree 14/2020, and, subsequently in the art. 17 bis (Provisions on the processing of personal data in the emergency context) of the decree law of 17 March 2020, n. 18 converted into law 24 April 2020, n. 27, whose effectiveness was lastly extended until 03/31/2022 (date of cessation of the state of emergency) by the Table Annex A (point 3), referred to in art. 16 paragraph 1 of the decree law of 24 December 2021, n. 221, converted with amendments into law 18 February 2022, n. 11";

- "Since, in the version of the TrakCare application installed at the Aosta hospital (TrakCare T2014), the parameter that governs the application of the dossier filters is system (this means that it is either active or not), in In the current version, it is not possible to select the activation of the filters with respect to Departments, Outpatient clinics/Services (therefore it is not possible to make a distinction between hospital services and territorial services). When the filters are deactivated, the TrakCare software is no longer able to apply the visibility rules indicated at the patient level, with the consequent situation that the information of those who have denied consent to the dossier, after which the previously set limitations on visibility will be restored". "This technical limit will be resolved in the new version, which will be installed in 2022 with the Consens manager which will allow for the separate management of • consent to the establishment of the DSE; • consent linked to the single event (dimming and de-dimming of the DCE); • a manager of document access policies (Privacy manager)" "This decision was implemented with Management Resolution no. 710 of 08/09/2021 concerning "Award of the "telematic procedure for the assignment of design, development and re-engineering services, application maintenance and support, management of the

operation of health information systems in use by the Local Health Authority of the Valley d'Aosta through a specific tender within the Framework Agreement for application services for public administrations stipulated by Consip - id 1881 - Lot 1 CIG: 861432805" in favor of the competitor RTI Accenture S.p.a., Accenture Technology Solutions S.r.l., Gpi S.p.a., Pricewaterhousecoopers Public Sector s.r.l." and with the signing of the related contract on 01/18/2022, which formally started in the month of February c.a. and whose implementation is expected within 8 months of taking charge";

- "The Director of SC Districts 1-2 Dr. XX (to which the Consultorio of Saint Pierre which concerns the case in question belongs) with note prot. XX of the XX (see XX) communicated that it had collected, with the support of SC Sistemi Informativi e Telecommunications, the data relating to the accesses made by Ms. XX on the dates indicated and that it had asked her for the reasons for this behavior (…). With subsequent note prot. XX of the XX (v...) communicated that he had verbally called the aforesaid XX to respect the observance of the regulation in force regarding privacy and at the same time proceeded, with note Prot. n. XX of the XX (...), to notify the SC Development of Human Resources of what happened, for any disciplinary measures. In order to avoid the recurrence of similar situations, Dr. XX also declared that she had taken the opportunity to sensitize all the personnel belonging to Districts 1 and 2 on the subject";

In attachment 7 to the acknowledgment note to the request for information, called "Motivations XX", on which Ms XX's handwritten signature is affixed, it is reported that she has accessed the file of the complainant, as well as her colleague, for " mere curiosity".

In the aforementioned note from the medical director of the aforementioned Company of the XX it was indicated that "In relation to the object, it is communicated that the art. 14 of the Legislative Decree 14/2020, has provided, among other things, indications concerning the processing of particular and judicial data in the current emergency moment. In essence, the provision aims to balance the right to the protection of personal data with the more general right to the protection of public health and safety, introducing an exceptional regime which allows certain subjects to carry out the processing of health data, including their communication. In this context, the subjects operating in the civil protection system (State, Regions, Autonomous Provinces of Trento and Bolzano, Local Authorities), their implementing subjects, the public and private structures of the National Health Service may, for reasons of public interest and for the diagnosis and assistance of the infected, communicate the personal data of the interested parties to each other. In the hospital context, this provision can translate into the possibility, for all doctors and nurses, to access the Trackare application for consultation and communication between them

of the personal data of patients hospitalized in the 3 hospitals, if those reasons of public interest exist and to ensure the diagnosis and health care of the infected in the emergency context following the COVID 19, provided for by the law". The note also goes on to highlight that "In substance and operationally: from 1:00 pm today, 03/17/2020, we are in a position to disable the Privacy functions that they manage, for the entire TrakCare site (therefore user profiles Doctors, Nurses, Administrative etc ...), the concepts related to the visibility of information. Basically, the visibility of the data will therefore be complete/general and no longer filtered on the basis of competence".

In the aforementioned note on the removal of the "privacy filters", the Company recalled "the need for correct and responsible use of the free access method, of which only the personnel concerned should be informed" and recalled "that the minimum measures must in any case be observed repeatedly the subject of corporate communications";

In relation to the results of the aforementioned preliminary investigation, the Office, with deed no. XX of the XX, notified the Local Health Authority of Valle d'Aosta (hereinafter Company), pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions referred to in article 58, par. 2, of the Regulation, inviting the aforesaid owner to produce defense 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 law no. 689 of 11/24/1981).

In particular, in the aforementioned note, the Office highlighted that the discipline dictated by art. 17-bis of the legislative decree no. 18/2020, referred to by the Company in the documentation sent, has not and could not have derogated from the data protection regulations which, as is known, are based on a European Regulation, but have provided for some simplifications in the processing and communication of data personal data between different data controllers only if the same are indispensable for the purpose of carrying out the activities connected to the management of the current health emergency and in any case in compliance with the principles set out in article 5 of the Regulation, adopting appropriate measures to protect the rights and of the freedoms of the interested parties.

In this regard, the Office also represented how the Authority has repeatedly highlighted the need to assess the applicability of the discipline referred to in the aforementioned art. 17-bis of the legislative decree no. 18 of 2020 on a case-by-case basis, drawing the attention of data controllers, including those operating in the health sector, to the fact that not all health data processing and communications can be traced back to this provision (see among many others, note of the 9 June 2020, web document n. 9429175). The Office therefore noted that the art. 17-bis d.l. no. 18 of 2020, cited by the Company as a provision

legitimizing the "possibility, for all doctors and nurses, to access the Trackare application for consultation and communication between them of the personal data of patients hospitalized in the 3 hospitals, as those reasons of public interest and to ensure the diagnosis and health care of the infected in the emergency context resulting from COVID 19, envisaged by the law", cannot be considered as a derogating rule from the present case of the obligation to acquire the consent of the interested party nor of compliance with the principles of lawfulness, correctness and transparency and of integrity and safety.

It was then noted that with reference to the processing of the personal data under examination, the same does not concern health services provided in an emergency, does not pertain to an interested party who has received health services related to Covid-19 and was not carried out by an operator for ensure health interventions related to the aforementioned pandemic, but out of "mere curiosity".

Given this, the Office disputed that the configuration of the health dossier chosen by the Company following the Covid-19 health emergency was carried out in violation of the basic principles of treatment pursuant to articles 5, par. 1, lit. a) and f), and of the articles 9, 25 and 32 of the Regulation. The violation of the aforementioned provisions makes the administrative sanction envisaged by art. 83, par. 4, lit. a) and par. 5, letter. a) of the Regulation.

With a note dated XX, the Company sent written defenses and asked to be heard, reiterating what has already been reported in the documents and highlighting, in particular, that:

- "the partial suspension of the privacy filters was immediately balanced by the maintenance of two distinct profiles (nurse/doctor) which allowed a very different depth of access from each other";
- "the Data Controller became aware of the aforementioned technical limits well before the event that is the subject of this proceeding and, therefore, by initiating a complex process of technological adaptation in advance, took steps to overcome the critical issues of the TrakCare T2014 version (system parameter which governs the application of the Dossier filters) by inserting technical specifications aimed at overcoming the limits of the current version in the tender for the new health information systems";
- "The AUSL wishes to reiterate how the choice to suspend the privacy filters has become indispensable for organizing and delivering - in a necessarily very short time - the activity both in the new Covid departments";
- "Health care personnel (doctors and nurses) who found themselves shifting in all COVID and non-COVID wards (which have become multi-specialist and/or multi-surgical wards), where patients assigned to different specialist structures were

hospitalized (e.g. Vascular Surgery + Pneumology + Neurology), he would no longer have had the possibility, in the light of the structure profile assigned (and, as mentioned, connected to the department to which he belongs), to access, according to the needs of the moment, the health information of TrakCare, nor, on the other hand, given the very high staff turnover in the COVID wards, real-time updating of the profiles was conceivable so that it was consistent with the performance of the activity in favor of the patients";

- "with reference to the interpretation and scope of art. 17-bis, the AUSL believes that, if the Legislator with the aforementioned provision, in the spirit of "simplification" has allowed various data controllers to be facilitated in the communication of data, it does not seem wrong to deduce as a fortiori the same and only Data Controller (AUSL) could be considered legitimately authorized to simplify the "consultation" of the data of which it was, in fact, owner by the AUSL operators involved in the management of the health emergency";
- "moreover, starting from the assumption that the exceptions introduced by art. 17 bis were valid for the performance of "activities connected to emergency management", the AUSL deems it necessary to ask itself which activity can be considered more "connected to emergency management" than the specific one of treating COVID patients";
- the "Company believes that the aforementioned list of reservations cannot be considered data relating to health, at least not in the strict sense";
- "access to the Dossier was voluntary, i.e. the operator - despite the precise instructions of the Management that accompanied the temporary easing of the filters - deliberately made an unjustified access";
- "In hindsight, the only purpose that in the present case moved the undersigned AUSL (i.e. the protection of public health), seems to reasonably be able to be traced back to the hypotheses of fulfillment of a duty, exercise of a legitimate faculty and/or state of necessity pursuant to art. 4, Law no. 689/1981".

The XX, via remote videoconference, was held, pursuant to art. 166, paragraphs 6 and 7 of the Code, the hearing of the Company, during which it reaffirmed what has already been declared in the documents and represented, in particular, that:

- "With the Covid-19 pandemic, the setting relating to the processing of personal data envisaged for the company health dossier constituted an obstacle to the performance of care activities, especially with reference to the analytical profiling of the roles of health workers. In particular, in the early stages of the emergency (March/April 2020) it was necessary to create new wards dedicated to the treatment of Covid-19 (almost ¾ of hospital wards), as well as to convert both medical and surgical

personnel to the service of these departments also in consideration of the absence of healthcare personnel due to the same Covid-19. This situation has led the Company's health and administrative departments to deem it necessary to eliminate the access filters to the health dossier, in order to guarantee the care of Covid-19 patients. This management was also maintained with the subsequent waves. This choice was made with a view to balancing the need for care and protection of personal data with reference to the state of emergency in progress at the time";

- "During this period, however, the Company made it clear to the operators of the need to limit access to the dossier exclusively if involved in the process of treating the data subjects, relying on their duties of confidentiality and service";
- "The process of restoring the health dossier management system according to the pre-pandemic rules was launched on 22 April 2022 and ended on 10 May 2022. This process made it necessary to verify the correct profiling of users";
- "The facts that are the subject of the proceeding took place in an outpatient clinic belonging to the Company, to which the ownership of the treatment is attributable. In this clinic, care was also provided for patients who had had Covid-19, although the present case refers to a non-Covid-19 patient";
- "The operator who logged in was an operator of an administration agency, to whom the facts object of the proceeding were reported. Subsequently, the contract with the aforementioned operator was not renewed. The Company has no reports of complaints to the Public Prosecutor's Office on the facts involved in the proceeding".

During the aforementioned hearing which took place via video link, the Company shared the screen in order to be able to show the health dossier application in use at the same, illustrating the functions present with the settings envisaged in the pre-pandemic period and those in force at the period of the facts in question, accessing with a profile similar to that of the aforementioned speech therapist in relation to a health dossier referring to a non-existent patient (test environment). As reported in the minutes of the hearing in the file, this presentation highlighted that with the application of the original "privacy filters" the operator (with a speech therapist profile) can only access the health services in which he is involved, while with the removal of the aforementioned filters could display the list of all services - with the indication of some details (not reports) relating to them (type of surgery, hospitalization, health conditions) - or even those with reference to which he was not involved in the treatment.

With a subsequent note of the XX, the Company sent a video certifying the aforementioned different ways of accessing the dossier shown during the hearing and a note from the company Synergie (staff agency) relating to the actions taken against

the manager of the access to the dossier in question (disciplinary complaint and written disciplinary warning).

2. Outcome of the preliminary investigation.

2.1. Legal framework of reference.

As a preliminary point, it should be noted that the processing of personal data must take place in compliance with the applicable legislation on the protection of personal data and, in particular, with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter, the "Regulation") and Legislative Decree no. 196 of 30 June 2003 (Code regarding the protection of personal data - hereinafter, the "Code").

With particular reference to the question in question, it should be noted that personal data must be "processed in a lawful, correct and transparent manner" (principle of "lawfulness, correctness and transparency" and "in such a way as to guarantee adequate security (...), including the protection, through adequate technical and organizational measures, from unauthorized or unlawful processing (principle of "integrity and confidentiality")" (Article 5, paragraph 1, letters a) and f) of the Regulation).

The Regulation then provides that the data controller implements "adequate technical and organizational measures to guarantee a level of security appropriate to the risk", taking into account, among other things, "the nature, object, context and purposes of the processing, as well as the risk of varying probability and severity for the rights and freedoms of natural persons" (Article 32 of the Regulation).

Taking into account inter alia the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing, both when determining the means of processing both at the time of processing itself the data controller must then implement appropriate technical and organizational measures, aimed at effectively implementing data protection principles, such as minimization and ensuring that they are processed, by default by default, only the personal data necessary for each specific purpose of the processing (Article 25 of the Regulation).

With reference to the treatments covered by the aforementioned complaint, the Guarantor has adopted the "Health Dossier Guidelines - 4 June 2015" (Provision of 4.6.2015, published in Official Gazette 164 of 17 July 2015, which can be consulted on www.gpdp.it web doc n. 4084632), in which a first framework of precautions have been identified, in order to outline specific guarantees and responsibilities, as well as necessary and appropriate measures and precautions to be placed as a guarantee for citizens, in relation to the processing of health data that concern, which, like the other provisions of the Authority, continue

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

In the aforementioned 2015 guidelines, the Guarantor specified that the health dossier, constituting the set of personal data generated by present and past clinical events concerning the data subject, constitutes a specific and additional processing of personal data compared to that carried out by the health professional with the information acquired during the treatment of the single clinical event. As such, therefore, it is configured as an optional treatment. In fact, the interested party must be allowed to choose, in full freedom, whether or not the clinical information concerning him is treated in a health dossier, also guaranteeing the possibility that the health data remain available only to the health professional who drafted them , without their necessary inclusion in that instrument. This means that if the interested party does not express his consent to the processing of personal data through the health dossier, the professional who takes care of him will only have access to the information provided at that moment by the interested party (e.g. collection of medical history, information relating to the examination of the diagnostic documentation produced) and those relating to previous services provided by the same professional. Similarly, in this circumstance, the ward/ambulatory health personnel will only have access to the information relating to the episode for which the interested party contacted that facility and to other information relating to any health services provided in the past to that subject by that department/outpatient clinic (so-called access to departmental vertical applications).

Following the full application of the Regulation (May 2018), with the provision of 7 March 2019, the Guarantor identified - by way of example - some treatments in the health sector for which it is still necessary to request the explicit consent of the interested party (art. 9, paragraph 2, letter a) of the Regulation), including those carried out through the health dossier (web doc. n. 9091942).

In the aforementioned Guidelines, the Guarantor, in order to avoid the risk of unauthorized persons accessing the information processed through the health dossier or of communicating health data to third parties by persons authorized to do so, specifically asked the data controllers of the treatment to pay particular attention to the identification of the authorization profiles and in the training of authorized subjects, since access to the dossier must be limited only to healthcare personnel who intervene in the patient care process and technical methods must be adopted for authentication of the dossier which reflect the cases of access to this tool specific to each healthcare 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 healthcare personnel may need to consult the healthcare dossier, for the treatment of the interested party and, based on this reconnaissance, identify the different access authorization profiles.

It is also represented that in the aforesaid Guidelines, the Authority considered that "the data controller must implement systems for access control also to the database and for the detection of any anomalies that could constitute unlawful processing, through the use of indicators of anomalies (so-called alerts) useful for guiding subsequent audit interventions. The controller must therefore prefigure the activation of specific alerts that identify anomalous or risky behavior relating to the operations performed by the persons in charge of processing (e.g. relating to the number of accesses performed, the type or time frame of the same)".

Since the declaration of the state of emergency approved by the Council of Ministers on 31 January 2020, many emergency regulatory acts have been adopted, which also contain provisions relating to the processing of health data carried out as part of the interventions relating to the aforementioned health emergency . The emergency provisions provide for emergency interventions which involve the processing of data and which are the result of a delicate balance between public health needs and those relating to the protection of personal data, in accordance with the provisions of the European Regulation for the prosecution of reasons of public interest in the public health sector (see Article 9, paragraph 2, letter i), of the Regulation).

With specific reference to the discipline dictated by art. 17-bis of the legislative decree no. 18/2020, referred to by the Company in the briefs in the proceedings, it is reiterated that this provision, within the limits permitted by the current legal framework, has provided for some "simplifications" in the processing and communication of personal data between different data controllers only if the same are indispensable for the purposes of carrying out the activities connected to the management of the current health emergency and in any case in compliance with the principles set forth in art. 5 of the Regulation, adopting appropriate measures to protect the rights and freedoms of the interested parties. As repeatedly reiterated by the Guarantor, this provision has not and could not have derogated from the provisions set out in the European Regulation for the protection of the fundamental rights of the interested party.

Therefore, it is reiterated that the processing of personal data connected to the management of the aforementioned health emergency must take place in compliance with the current legislation on the protection of personal data and, in particular, in compliance with the principles and limits applicable to the processing, referred to in 'art. 5 of the Regulation, according to which

the data must be processed lawfully, correctly and transparently in relation to the data subject ("lawfulness, correctness and transparency"), "collected for specific, explicit and legitimate purposes" ("purpose limitation") and, in any case, "adequate, pertinent and limited to what is necessary with respect to the purposes for which they are processed" (data minimization principle).

Compliance with these principles in the processing of personal data carried out in the aforementioned health emergency from Covid -19 was moreover repeatedly referred to and evaluated by the Authority in the numerous opinions rendered on the regulatory acts regulating information systems implemented urgently for the detection of infections from Covid-19, for the booking and registration of vaccinations, for the national contact tracing system (App Immuni) and for the generation and control of the Covid-19 green certifications.

Finally, it should be noted that, in the light of the Regulation, "data relating to health" are considered: personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information relating to his or her state of health (Article 4, paragraph 1, no. 15 of the Regulation). Recital no. 35 of the Regulation in fact specifies that data relating to health "include information on the natural person collected during his registration in order to receive health assistance services"; “a specific number, symbol or element attributed to a natural person to uniquely identify him or her for health purposes”.

2.1 Scope of processing and nature of the data processed.

As a preliminary point, it should be noted that, according to what is indicated by the Company itself in the documents, the treatments in question, which took place in a company clinic, are attributable to the ownership of the same.

In the light of what emerged in the preliminary documents, the Company has intentionally chosen to adopt an administrative act with which to order the "removal of privacy filters" in the information system that manages the company health dossier, in the belief that this measure would have simplified management of patients during the pandemic.

The removal of the aforementioned filters resulted in:

- the activation of the health dossier for all the patients of the Company, which coincide with those of the Region, even if they have expressly denied consent to use the dossier or have never provided it;
- the possibility that the dossier was consulted, albeit with different depths of access, by all company healthcare operators regardless of their involvement in the treatment path of the interested party.

It should also be noted that although the aforementioned company choice was made in relation to the Covid-19 emergency, the removal of the aforementioned filters did not only concern patients suffering from this pathology, but all those belonging to the Company and its branches (such as the structure where the access in question was made) and was not limited only to health services rendered in an emergency, but to all those provided by the Company from March 2020 to May 2022.

Given this, it is noted that the choice made by the Company actually allowed Ms XX to access the information relating to the health services provided to the complainant (Ms XX's colleague) to which she would not have had access if she had not been the removal of the aforesaid "privacy filters", this because the complainant had not consented to the use of the company health dossier and the aforesaid operator was not involved in the treatment path of the interested party.

In light of the foregoing, the information relating to the complainant accessed by Ms XX qualifies as health data. Although in fact the presence of some filters has allowed the aforementioned healthcare worker to see only the list of episodes already carried out or booked by the interested party with the indication of the type of service, and not also to "consult the reports", such information is in any case relating to the health of the claimant and therefore qualify as data on the health of the same.

With the profile of the aforesaid operator it was in fact possible to access information relating to the type of service provided, the clinic providing it, any hospitalization and elements relating to the health conditions of any patient of the Company regardless of the will of the subject to whom they referred (denial of consent to the dossier or absence of consent) and by the actual involvement in the treatment path of the operator.

Therefore, it should be noted that the choice made by the Company has in fact made the health dossiers of all its clients accessible, which, as stated in the deeds, coincide with those of the Region (the Company is the only one present in the Valle d 'Aosta), regardless of the will of the same, the involvement in the treatment path of the healthcare operator and the circumstance that the healthcare service was actually provided to a Covid-19 patient.

2.2 The consent of the interested party and principles of lawfulness, correctness and transparency and data protection from the design and by default.

As highlighted above, with the provision of 7 March 2019 and in the subsequent provisions, including of a sanctioning type, adopted on the matter, the Guarantor noted that the legal basis of the processing of personal data carried out through the health dossier is the explicit and informed consent of the interested party (Article 9, paragraph 2, letter a) of the Regulation).

An examination of the documents in the file shows that the aforementioned "removal of the privacy filters" on the company

health dossier determined, for each company/regional client, the creation and accessibility of the health dossier regardless of the will expressed by the interested parties and even contrary to an explicit refusal of the same, as in the case of the complainant.

In this regard, it is important to highlight that the legislative interventions adopted during the pandemic to facilitate the management of the same have confirmed the need for the consent of the interested party also with reference to specific emergency treatments such as that relating to the online reporting of tests for Covid- 19 (DM 2 November 2020 which refers to the dPCM 8 August 2013) or to consult the electronic health record for treatment purposes, an instrument that has similar purposes to the health dossier (see art. 12 legislative decree n. 179/2012 in relation to the changes made by Article 11, Legislative Decree No. 34 of 2020).

Having said that, we reiterate what has already been noted with the note of the XX, namely that the art. 17-bis of the legislative decree no. 18 of 2020, cited by the Company as a provision legitimizing the "possibility, for all doctors and nurses, to access the Trackare application for consultation and communication between them of the personal data of patients hospitalized in the 3 hospitals, as those reasons of public interest and to ensure the diagnosis and health care of the infected in the emergency context following the COVID 19, envisaged by the law", cannot be considered as a derogating rule from the obligation to acquire the consent of the interested party.

The aforementioned emergency regulation has in fact provided for some simplifications (e.g. in relation to the information to be provided pursuant to article 13 of the Regulation or to the authorizations pursuant to article 2-quaterdecies of the Code) reiterating the need to respect the principles to art. 5 of Regulation (EU) 2016/679, including that of lawfulness, i.e. identifying the correct legal basis of the processing, and adopting appropriate measures to protect the rights and freedoms of the interested parties.

The removal of the so-called "privacy filters" carried out by the Company resulted in a violation of the aforementioned principles and in particular those of lawfulness, correctness and transparency, as the company health dossiers of the entire assisted regional population were:

- made even contrary to the will of the interested parties or in the absence of their explicit consent;
- made accessible by default also to healthcare personnel not involved in the patient's treatment path, without the patients themselves ever being informed.

The violation of the principle of correctness and of the connected principle of proportionality of the treatment is also evident with reference to the circumstance that the removal of the so-called "privacy filters", did not only concern the health services provided in an emergency or the dossiers of the interested parties to whom health services related to Covid-19 were to be provided, but also all the patients belonging to the Company - even those not currently under treatment - and with reference to any course of care undertaken by them.

From this it can be seen that the Company, on the occasion of the aforementioned health emergency, knowingly removed the measures, also required by the aforementioned Guidelines of the Guarantor, which limited access to the file to only the health personnel who treat the interested party. This choice effectively allowed Ms XX, not involved in the provision of emergency healthcare services linked to the aforesaid virus, to make repeated accesses to the dossier of an assisted person, as well as a colleague, without a suitable prerequisite of lawfulness, but only for reasons of "mere curiosity" (accesses from March 2021 to December 2021).

The case in question demonstrates that the aforesaid changes to the configuration of the company file made it possible for a health professional working at the Company to access the health dossier even of interested parties who were not being treated at the Company at that time or in any case at the owner of the account and who had never given their consent to the file (or, as in the present case, consent to the file had even been expressly denied) in violation of the basic principles of treatment pursuant to articles 5, par. 1, lit. a) and f) and 9 of the Regulation, as well as the principle of data protection from the design (privacy by design) and by default (privacy by default) (art. 25 of the Regulation.

2.3 Authorization profiles for access to the health dossier and alert systems.

As a preliminary point, it should be noted that the rules regarding the accessibility of the dossier adopted by the Company in the pre-pandemic era, according to which "doctors and other health professionals belonging to different specialized Structures and/or disciplines could not, in fact, have access the medical records and health data of patients hospitalized in COVID wards (formally assigned to the Pulmonology department) or in multi-specialist non-COVID wards and therefore would not have been able to adequately assist patients" are the result of a choice by the same Agency. On this point, the Authority has in fact repeatedly recalled the need to limit access to the dossier to only healthcare personnel who actually intervene in the patient care process regardless of the department in which the same is assigned, calling on the owner to adopt technical methods of authentication to the dossier that reflect the cases of access to this tool specific to each healthcare facility.

It should also be noted that the problem described by the Company, according to which at the time the aforementioned filters were deactivated, "the TrakCare software is no longer able to apply the visibility rules indicated at the patient level, with the consequent situation that temporarily display, i.e. limited until the state of emergency persists, also the information of those who have denied consent to the dossier", after which the limitations on visibility previously set will be restored", does not depend on the "rigidity" of the legislation on protection of personal data, but by the characteristics of the system chosen by the Company itself. Indeed, updating the system has allowed the Company to overcome this difficulty.

The choice made by the Company to "disable the Privacy functions which manage, for the entire TrakCare site (therefore user profiles for Doctors, Nurses, Administrative staff, etc...), the concepts linked to the visibility of information. Basically, the visibility of the data will therefore be complete/general and no longer filtered on the basis of competence", not only does it not find foundation, as already represented, in the aforementioned art. 17-bis of Legislative Decree no. 18 of 2020, but it was operated in such a way as to allow access to the health dossier also by health professionals not involved in the health emergency and with reference to all health services and not just emergency ones.

As already highlighted, the configuration of the health dossier envisaged by the Company in the emergency period effectively provided for a single access profile (albeit with different access depths), thus allowing all health personnel to consult the health dossiers of any patient had been under treatment at the Company regardless of the circumstance that the subject who logs on is involved in the treatment path of the interested party and that the latter has given his consent to the processing of data carried out through the dossier.

In derogating from the limitations relating to access to the health dossier dictated by the application of the regulations on the protection of personal data, the Company, while declaring that "the visibility of the data will therefore be complete/general and no longer filtered on the basis of competence", has not even adopted a system for detecting any anomalies that could constitute unlawful processing, or the use of indicators of anomalies (so-called alerts) aimed at identifying anomalous or risky behavior relating to the operations carried out by subjects authorized to process (e.g. number of accesses performed, type or time frame of the same), useful for guiding subsequent audit interventions, in violation of the principles of integrity and confidentiality of personal data (Article 5, paragraph 1, letter f), of the Regulation).

According to what was declared in the documents, the system of restoring the "pre-pandemic rules" in the health dossier was started on 22 April 2022 and ended on 10 May 2022; therefore, it emerges that the removal of the so-called "privacy filters" has

been operational for over two years (50 months), having started in March 2021 and the aforementioned "technical limits" of the information system used for the health dossier were belatedly detected. The Company's choice "to suspend the privacy filters" as "indispensable to organize and deliver - in necessarily very short times - the activity in the new Covid departments" therefore extended beyond the first emergency phase.

3. Conclusions.

In the light of the assessments referred to above, taking into account the statements made by the data controller during the preliminary investigation and considering that, unless the fact constitutes a more serious crime, anyone who, in a proceeding before the Guarantor, falsely declares or certifies or circumstances or produces false deeds or documents, it is liable pursuant to art. 168 of the Code "False declarations to the Guarantor and interruption of the execution of the duties or exercise of the powers of the Guarantor" it is stated that the elements provided by the data controller in the defense briefs relating to the aforementioned proceedings do not allow the findings notified to be overcome by the Office with the deeds of initiation of the proceedings for the adoption of corrective and sanctioning measures, since none of the cases provided for by art. 11 of the Regulation of the Guarantor n. 1/2019.

For these reasons, the illegality of the processing of personal data carried out by the Local Health Authority of Valle d'Aosta is noted with reference to the procedure initiated following the complaint, in the terms set out in the justification, in particular, for having processed personal data in violation of the articles 5, par. 1, lit. a) and f), 9, 25 and 32 of the Regulation.

In this context, considering that disciplinary measures have been taken against the author of the access and that the measures for accessing the pre-pandemic health dossier described above have been restored since May 2022, the conditions for the adoption of the corrective measures pursuant to art. 58, par. 2, of the Regulation.

4. Adoption of the injunction order for the application of the pecuniary administrative sanction and accessory sanctions (articles 58, paragraph 2, letter i and 83 of the Regulation; article 166, paragraph 7, of the Code).

The violation of the articles 5, par. 2, lit. a) and f), 9, 25 and 32 of the Regulation, caused by the conduct of the Local Health Authority of Valle d'Aosta, is subject to the application of the administrative fine pursuant to art. 83, par.4 and 5, of the Regulation.

Consider that the Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, has the power to "impose a pecuniary administrative sanction pursuant to article 83, in addition to the [other] [corrective] measures

referred to in this paragraph, or instead of such measures, according to the circumstances of each single case" and, in this context, "the College [of the Guarantor] adopts the injunction order, with which it also orders the application of the ancillary administrative sanction of its publication, in whole or in part, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code" (art. 16, paragraph 1, of the Guarantor's Regulation no. 1/2019).

The aforementioned pecuniary administrative sanction imposed, depending on the circumstances of each individual case, must be determined in the amount taking into account the principles of effectiveness, proportionality and dissuasiveness, indicated in art. 83, par. 1, of the Regulation, in the light of the elements provided for in art. 85, par. 2 of the Regulation in relation to which for both proceedings it is observed that:

- the Authority became aware of the event following a complaint (Article 83, paragraph 2, letter h) of the Regulation);
- the illicit accesses concerned the health dossier of a patient who was at the same time an employee of the Company by a health professional who was not involved in the treatment process of the same and against whom a disciplinary procedure was initiated (art. 83, paragraph 2, letters a) and b) of the Regulation);
- the accesses to the complainant's health file made for reasons of "mere curiosity" took place in the space of 9 months from 03/15/2021 to 12/06/2021 by a health worker who, in addition to not being involved in the treatment path of the interested party, she was not even employed in the provision of emergency health services linked to the aforementioned virus (Article 83, paragraph 2, letter a) of the Regulation);
- the aforesaid accesses were possible since the removal of the aforesaid "privacy filters" effectively allowed Ms XX, who was not involved in the treatment of the complainant and in the provision of emergency health services linked to the aforesaid virus, to carry out repeated accesses to the dossier of a client, as well as a colleague, without a suitable prerequisite of lawfulness, but only for reasons of "mere curiosity" (Article 83, paragraph 2, letters a) and d) of the Regulation);
- the Company has consciously chosen to proceed with the removal of the so-called "privacy filters" for all company health dossiers of the entire assisted regional population determining the activation of the health dossier for all the Company's clients even if they have expressly denied consent to use the dossier or have never given it , as well as the possibility that the dossier was consulted, albeit with different access depths, by all company healthcare operators regardless of their involvement in the treatment path of the person concerned (Article 83, paragraph 2, letter b) and d) of the Regulation);
- the aforementioned company choice, although it was made in relation to the Covid-19 emergency, did not only concern

patients suffering from this pathology, but all those belonging to the Company and its branches (over 120,000 affected) and is not been limited only to health services rendered in an emergency, but to all those provided by the Company from March 2020 to May 2022 (Article 83, paragraph 2, letter a), b), c) and d) of the Regulation) ;

- in derogating from the limitations relating to access to the health dossier dictated by the application of the regulations on the protection of personal data, the Company has not adopted a system for detecting any anomalies that could constitute unlawful processing, or the use of indicators of anomalies (so-called alerts) aimed at identifying anomalous or risky behavior relating to the operations carried out by the subjects authorized to process the data (e.g. number of accesses performed, type or time frame of the same), useful for guiding subsequent audit interventions, in violation of the principles of integrity and confidentiality of personal data (Article 83, paragraph 2, letter d) of the Regulation);

- in removing the aforementioned "privacy filters", the Company had recalled "the need for correct and responsible use of the free access method, of which only the personnel concerned should be informed" (Article 83, paragraph 2, letter c) of the Regulation);

- the recovery system in the management of the health dossier of the "pre-pandemic rules" was launched on 22 April 2022 and ended on 10 May 2022 (Article 83, paragraph 2, letters a) and c) of the Regulation) .

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 5, letter. a) of the Regulation, for the violation of the articles 5, par. 1, lit. a) and f) and 9 of the Regulation in the amount of 40,000 (forty thousand) for the proceeding initiated following the complaint as a pecuniary administrative sanction withheld, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary sanction of publication on the Guarantor's website of this provision should be applied, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Regulation of the Guarantor n. 1/2019, also in consideration of the type of personal data subject to unlawful processing.

Finally, it should be noted that the conditions pursuant to art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

ALL THIS CONSIDERING THE GUARANTOR

declares the illegality of the processing of personal data carried out, in both the procedures described, by the local health authority Valle d'Aosta, for the violation of the art. 5, par. 1, lit. a) and f), 9, 25 and 32 of the Regulation in the terms referred to

in the justification.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to Local Health Authority Valle d'Aosta, C.F. 91001750073, to pay the sum of 40,000 (forty thousand) euros as a pecuniary administrative sanction for the aforementioned violations according to the methods indicated in the annex, within 30 days of the notification in the 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 penalties imposed.

ENJOYS

to the aforementioned Company, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sums of 40,000 (forty thousand) euros according to the methods indicated in the annex, within 30 days of notification of this provision, under penalty of adopting the consequent executive acts pursuant to art. 27 of the law n. 689/1981.

HAS

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

Pursuant to art. 78 of the Regulation, of the articles 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision it is possible to lodge an appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the appellant resides abroad.

Rome, 10 November 2022

PRESIDENT

Station

THE SPEAKER

Zest

THE SECRETARY GENERAL

Matthew