[doc. web no. 9529527]

Injunction against the South East Tuscany Local Health Authority - 17 December 2020

Register of measures

no. 278 of 17 December 2020

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 natural persons 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 no. 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 Guarantor's office for the protection of personal data, doc. web no. 1098801;

Supervisor Prof. Geneva Cerrina Feroni;

WHEREAS

1. The violation of personal data and the preliminary investigation

As part of the preliminary investigation carried out with reference to a report from a general practitioner on the initiative health model adopted by the Azienda USL Toscana Sud Est (hereinafter Company) and in the light of the information provided by the

same at the request of the Office (note dated 13.7.2018, prot. n. 21012, acknowledgment dated 24.8.2018), on 27 November 2018 an inspection was carried out at the aforementioned Company aimed at verifying compliance with data protection regulations personal data, with particular reference to the processing of particular categories of data carried out in the context of the c.d. “initiative health care”.

During the aforementioned inspection, it was found that:

- the care approach model of the c.d. "Health initiative", followed throughout Tuscany, is based on the anticipation of services to certain categories of patients, in order to prevent morbid events. This model sees the participation of various actors of the regional health service and in particular general practitioners (GPs) and the clinics of local health authorities (integrated clinical networks), who operate as independent data controllers, under organizational coordination of the territorially competent health authority. The model is realized through the impulse of the GP, who, in the so-called "enrollment phase", selects, among its patients, those suffering from chronic pathologies identified at a regional level (e.g. diabetes, heart failure) and offers them Individual Assistance Plans (PAI), characterized by the offer of a calendar of services strictly connected to the pathologies suffered by the patient. If the patient decides not to join this plan, he will still be able to take advantage of the services offered by the regional health service, as well as access the prevention campaigns;

- the healthcare model promoted by the Company has had a different structure over time. In a first phase, which ended in 2017, GPs sent the Company only the total number of patients enrolled in relation to the various chronic conditions indicated (e.g. diabetes). If the total number of enrolled patients deviated significantly from the regional average (verification of the plausible number as prevalence), the Hospital carried out random checks, as part of the supervisory functions assigned to it. Instead, starting from 2018, it was decided to expand the range of information that GPs had to send to the Company as part of the healthcare assistance model promoted by the same. To this end, the Company has sent GPs the updated list of their clients in an Excel table (in zip format with password for opening the file). After acquiring a specific informed consent from the interested parties (in documents), the GPs proceeded to transmit the aforementioned list to the Company, after reporting, next to the name of each patient, the possible presence of one or more of the conditions morbid cases for which it was intended to enlist the same;

- the sending of such data, by the GPs, had been considered as a condition for the recognition to the doctor of a portion of the funding envisaged by the collective agreements (compliance with the prevalence targets);

- the legal basis for the communication of particular categories of personal data from GPs to the Company has been identified in the consent of the interested party and in file no. 7, attachment B) to the Regulations for the processing of sensitive and judicial data of the Tuscany Region;

- for the purposes of the aforementioned enrollment, the GPs proceeded, by querying their own database, choosing the individual patients affected by the pathologies indicated by the Hospital. Having identified the patients to be enrolled, the GP proposed to the patients, on the occasion of the first contact, or with an active recall, an individual assistance plan (PAI);

- until 2018, the GP communicated to the Company only the total number of PAIs activated and the global number of specialist services that the Company itself would subsequently have to guarantee based on the PAIs activated;

- subsequently a new procedure was adopted which, unlike in the past, provided for the sending of the names of the enrolled patients (and no more than the total number). According to this new procedure, the GPs saved the aforementioned Excel table with the data of the patients enrolled on a removable support of their property (pen drive) and delivered the aforementioned support to the district doctor, who in turn saved the Excel file on his pc and return the removable media to the doctor. The district doctor then proceeded to send the file, via e-mail, to the district doctor in charge of the provincial area. Subsequently, this doctor forwarded, again via e-mail to the Regional Administrative Technical Support Body (ESTAR), the Excel files he had received from the various district doctors, attaching them, in zip format with password for opening (message in file). No losses or thefts of the aforementioned removable media used by the GPs for communicating the data of the enrolled patients to the Company have been reported;

- ESTAR was designated by the Healthcare Company as external data processor in 2016 (Prot. 0142457 dated 03/10/2016 in documents). At the time of the inspections, the Healthcare Company, as part of the regional privacy table in which the representatives of the other healthcare companies of the Tuscany Region participate, was proceeding with the revision of this designation, in order to bring it into line with the new provisions dictated by the Regulation ;

- ESTAR, after receiving the aforementioned Excel files from the referring district doctors for provincial areas, consolidated this information and entered it in a corporate data warehouse. ESTAR then made available to the Company a data collector (data mart) relating to the progress of the enrollment process, by pathology and by doctor, which allowed the Company to carry out the aforementioned prevalence calculation (verification of the number plausible as prevalence);

- at the time of entering the data into the data warehouse by ESTAR, the acquired information was deprived of the directly

identifying data (name and surname) by associating, to each enrolled client, the unique regional code also used to fulfill the information debts towards the Region and the Ministry of Health. The monitoring, evaluation, management and control activities carried out by the Company on the aforementioned data warehouse refer to those described in sheet no. 39, attachment B) to the Regulations for the processing of sensitive and judicial data of the Tuscany Region. The aforementioned data warehouse could be accessed by authorized Company employees, through specific authentication credentials;

- the data described above have not been transmitted to the Tuscany Region;

- with regard to the treatments described above, the Healthcare Company has not carried out an impact assessment pursuant to art. 35 of the Regulation;

- furthermore, the retention time of the data collected through the aforementioned healthcare projects on the part of the doctors and the Company has not been defined;

- at the date of the inspections (November 27, 2018) the Register of treatment activities pursuant to art. 30 of the Regulation, which appeared to still be in a working version.

With an e-mail dated December 3, 2018, the Healthcare Company supplemented the documentation acquired during the aforementioned assessment, by sending a copy of the register of processing activities adopted on November 30, 2018, pursuant to art. 30 of the Regulation.

In relation to the results of the aforementioned preliminary investigation, the Office, with deed no. 10618 of 27 March 2019, notified the USL Toscana Sud Est Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in article 58, paragraph 2, of the Regulation, inviting the aforesaid holder 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 n. 689 of 11/24/1981).

In particular, the Office, in the aforementioned deed, represented that:

- in our legal system there is no specific definition and regulation of the so-called “initiative health/medicine”. Nonetheless, this term is present in numerous guidelines and planning acts of the Ministry of Health and the Regions. From the analysis of these documents, it is evident that "initiative medicine" means a care model oriented towards the "active promotion" of the health of the individual, especially if affected by chronic diseases or disabilities, and towards empowering people along their path care (source Ministry of Health http://www.salute.gov.it/portale/temi/p2_6.jsp?id= 496&area=Cure%20 primarie&menu=cure, see,

among many references, Ministry of Health, General Assembly of the Superior Health Council, "Telemedicine - national guidelines", 10 July 2012, see par. 2.3.2, Decree 02 April 2015, n. 70 - Regulation defining the relative qualitative, structural, technological and quantitative standards to hospital assistance, Agreement between the Government, the Regions and the autonomous Provinces of Trento and Bolzano on the project lines for the use by the Regions of the restricted resources pursuant to article 1, paragraphs 34 and 34 bis, of law 23 December 1996, no. 662 for the achievement of priority objectives of national importance for the year 2014);

- as highlighted in the report of the operations carried out, on the basis of an initiative promoted by the Company, the GPs have selected, among their patients, those affected by certain chronic pathologies identified at a regional level (e.g. diabetes, heart failure) (so-called Recruitment phase) and they proposed individual assistance plans (PAI), characterized by the offer of a personalized performance calendar, according to the pathologies suffered. Initially, the aforementioned doctors communicated to the Company only the total number of patients enrolled. Starting from 2018, on the other hand, the GPs, on the instructions of the Company, have compiled an Excel file containing the personal details of the patients registered with each doctor, highlighting, only for the patients enrolled, the presence of one or more of the morbid conditions for which it was intended to offer them a PAI (data in the table: name, surname, date of birth and tax code of the assisted person);

- the adoption of this procedure has led to the collection and processing of health data, in order to create, with reference to specific pathologies, a health risk profile of the person concerned and has therefore configured a treatment by the GP autonomous with respect to the main one aimed at the care of the patient based, at the time of the facts, on informed consent) and, since 2018, by the Company, a treatment of personal data on the health of patients, based on the consent of the interested party acquired through the model called "European regulation for the protection of natural persons with regard to the processing of personal data (n. 2016/679 RGPD) - Information pursuant to articles 13 and 14 of the Regulation" (in documents), created by the Company, in its capacity as data controller, and provided to the GPs so that it could be returned to the patient upon enrollment;

- in light of the nature of the data processed and the number of interested parties, the processing described above, carried out by the Company since 2018, falls within the cases in which the owner cannot ignore an impact assessment on data protection, pursuant to the provisions of the GDPR and the criteria identified by the Group art. 29 in the Guidelines concerning "The assessment of the impact on data protection as well as the criteria for establishing whether a treatment "may present a high

risk" pursuant to Regulation 2016/679" (n. 248 adopted in amended form on 04.10.2017 ; on this point see also the software - free and freely downloadable from the site www.cnil.fr (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la -cnil) which offers a guided path to the implementation of the DPIA, according to a sequence compliant with the indications provided by the WP29 in the Guidelines on the DPIA). In this regard, it was acknowledged that the aforesaid assessment had not been carried out in consideration of the fact that the project had been launched prior to the date of full application of the European Regulation;

- the treatment object of the preliminary investigation, not being strictly necessary for the purposes of treatment pursued by the various data controllers involved, was correctly carried out after obtaining the informed consent of the interested party (articles 9, paragraph 2 letters a) and h), 13 and 14 of the Regulation). The informed consent model, acquired as part of the inspection and relating to the processing activities implemented by the Company with reference to initiative healthcare, was however lacking in some of the information elements required by the aforementioned articles 13 and 14 of the Regulation, such as: the retention period of personal data, the rights recognized by the Regulation to the interested parties, the right to lodge a complaint with the Supervisory Authority and the contact details of the data controllers and the data protection officer. Furthermore, the aforementioned information model did not provide clear indications regarding the treatment carried out by the Regional Health Agency "for purposes of monitoring and assessing the quality of assistance", with particular reference to the indications relating to the legal basis of the treatment;

- at the time of the inspection, the Company had not yet adopted a register of the processing activities carried out by the same (pursuant to article 30 of the GDPR), which was only formalized subsequently on 30 November 2018;

- with specific reference to the procedure for sending the name data of patients enrolled by GPs, adopted starting from 2018, the Company should have implemented adequate technical and organizational measures to guarantee a level of security proportionate to the risk, which can include, among others, pseudonymisation, encryption of personal data and measures capable of ensuring, on a permanent basis, the confidentiality, integrity, availability and resilience of processing systems and services. The treatment methods identified during the inspection (GPs saving the Excel table on a removable support -pen drive- belonging to them, delivering the support material to the district doctor, saving the Excel file on the doctor's PC district and sending of the same - attached to an e-mail - to the referring district doctor for the provincial area, subsequent sending by the latter of the files received from all the district doctors to ESTAR, attaching them - in zip format with password for opening

an e-mail message) do not respect the principle of integrity and confidentiality and do not guarantee the security of the processing (articles 5, paragraph 2, letter f) and 32 of the Regulation);

- the designation as data processor of the company ESTAR, shown at the time of the inspection (Prot. 0142457 of 03/10/2016) and relating to all the processing activities carried out by the aforementioned body on behalf of the Healthcare Company, is found to be unsuitable with respect to the provisions of art. 28 of the Regulation as it did not indicate, in an analytical way, the specific tasks assigned and did not provide precise instructions in relation to the multiple treatments carried out by the Body, including those relating to self-initiated medicine.

In the aforementioned deed of 12 March 2019, the Office therefore considered that the Company had processed the personal data of data subjects who adhered to the "initiative health care" model in violation of:

- the right of the interested parties to receive - at the time of data collection - all the information pursuant to articles 13 and 14 of the Regulation;

- the obligations of the holder, with regard to the impact assessment on the protection of personal data pursuant to art. 35 of the Regulation;

- of the obligations of the owner, in order to respect the basic principles of the treatment pursuant to art. 5, par. f) of the Regulation and of the security of the treatment referred to in art. 32 of the Regulation;

and more generally, with reference to the complex of treatments carried out by the Company, in violation:

- the obligation to keep the register of processing activities pursuant to art. 30 of the Regulation;

- the obligations of the data controller regarding the correct designation of ESTAR as data processor pursuant to art. 28 of the Regulation, punctually identifying the tasks and instructions with reference to the multiple processing activities carried out by the Organization on behalf of the Company.

With a note dated May 22, 2019, the Company asked to be heard by the Authority and sent its defense briefs, in which, in particular, it was represented that:

a) "in the months following July 2018, there were no further transmissions by GPs to this Hospital of lists with the names of patients enrolled in 2018 (with the exception only of the Siena area, where some data were transmitted on 4 September, due to the absence of the referring district doctor) and that to date the new data collection procedure for 2019 has not yet been started";

b) it has been envisaged that "for 2019, GPs will communicate the data in aggregate and anonymous form, indicating only the total number of patients enrolled in relation to the various chronicities identified, without their names or in any case other personal data";

c) it was decided to "start the activities for the adoption, also at ESTAR, of specific organizational, technical and security measures (...) aimed at limiting any form of use or processing of personal data relating to enrolled patients referred to in lists acquired during 2018";

d) to want to "start the activities necessary to cancel the copies of the aforementioned personal data kept by the district doctors of this Company";

e) with specific reference to the information to be provided to the interested party, "as a result of the inspection (...) (there have been prepared) the new information and consent forms relating to the processing of personal data of patients who intend to confirm or carry out the adherence to the initiative Healthcare model for the year 2019 (...) and will soon be made available to GPs with the communication relating to the operating instructions that will be issued by this Company for carrying out the initiative Healthcare activities for the 2019. These instructions will also provide that the participating doctors will have to communicate to the Company only the aggregate data relating to the total number of patients enrolled for each of the identified pathways". "During this period of transition from the old to the new regime, as known, the previous provisions of Legislative Decree no. 196/2003 on the subject of information, as well as consent and other conditions for the lawfulness of processing, both general and specific with regard to the health sector (...), so it seems reasonable to believe that, also considering the framework of uncertainty at the regulatory level, the information and consent forms prepared in the first months of 2018 could still not be fully aligned with the new provisions of the Regulation";

f) with specific reference to keeping the register of processing activities, "at the time of the inspection of 27 November 2018 (...) this Company was in possession of a version of the register of treatments still in progress, concerning the treatments common to the companies territorial and hospital services, the result of the work carried out in the context of the "Regional privacy table/Regional health service bodies and companies", and had then completed and formally adopted the definitive version of this register, with the integration of the further treatments pertaining to the 'Company, the following 30 November";

g) with specific reference to the designation of ESTAR as data controller, the "Company had in any case attributed to ESTAR the designation and obligations of data controller pursuant to the previous art. 29 of the Privacy Code, according to the scheme

prepared by the Tuscany Region, which already contained various elements corresponding, in essence, to those provided for by art. 28 of the Regulation" and "on 13 November 2018 (that is, before the inspection), this Company had already resolved to proceed with the signing of the new scheme which was then formalized at the end of the year (in any case before the notification of the alleged violation)";

h) with specific reference to the preparation of an impact assessment, the "Company did not consider at the time to proceed with an impact assessment, as the personal data processing activity in question had in any case been configured and started before the application of the Regulation". The "Company had indicated its intention to proceed instead with an impact assessment regarding the possible technological developments of the procedure for sending the data in question via a platform technically managed by ESTAR, also in the light of the provision published in that period by this Authority concerning the list of types of processing subject to the requirement of impact assessment pursuant to art. 35, par. 4, of the Regulation";

i) with specific reference to the obligations of the holder regarding the security criteria, the "remarks made regarding the procedure followed in 2018 are currently to be considered outdated in the light (...) (of) the decision of this Company to provide for 2019 a communication by GPs only of aggregated and anonymous data referring to the total number of patients enrolled for the indicated courses and to adopt some specific measures aimed at making the data previously collected unusable" and that "moreover, there are no losses or thefts or in any case, security incidents resulting from the operation described above which, in the limited period of time in which it was implemented, although it could certainly be perfected in order to raise the security levels ";

On February 3, 2020, the Company renounced the hearing and integrated the documentation relating to the treatment in question, representing the additional activities carried out in the context of the so-called "initiative health care", highlighting, in particular, that:

a) it was envisaged that "each GP, as data controller, at the time of the first contact with the patient to confirm membership or for a new enrollment in the "Initiative Healthcare" model of care (therefore, both for patients already enrolled in 2018, and for those enrolled in 2019), release the information to the interested party and acquire their consent on the basis of the new forms prepared by the Company";

b) it was established that "the communications from the GPs adhering to the Healthcare initiative to the Hospital concern only the total number of patients enrolled in relation to the various chronicities identified, without their names or in any case other

personal data" ;

c) "as regards the nominative data of the enrolled patients referred to in the lists transmitted by the GPs during 2018 and kept by the district doctors employed by the Company, this Company has in any case also acquired from the latter a formal written attestation from the occurred cancellation of each copy of the same data, confirming what is indicated in point 2, second paragraph, third line, of the defense briefs. In this regard, it should be noted that the certificates received are kept in the records of this Company and that they can be made available to this Office, where deemed necessary";

d) “the Region of Tuscany, in consideration of the importance of the welfare model called "Initiative Health", has activated the institutional process for the integration into the regional legislation of a complete regulation of this innovative healthcare modality".

2. Outcome of the preliminary investigation.

The assessment carried out by the Office and the subsequent preliminary investigation concerned the processing of personal data carried out by the Azienda USL Toscana Sud Est within the so-called "Initiative healthcare model".

This model, although not regulated by any regulatory act at the national level, has been a reference organizational-welfare model at the regional level since 2009, which has had - over time - various forms and application denominations (e.g. chronic care model). These models were created in order to favor "a methodological approach to taking charge and the process of patient care" which translates into an "active and periodic recall of the patient to subject him to educational and clinical assistance activities, aimed at correcting lifestyles, empowerment, early diagnosis” (declarations present in the documentation in the file). The assistance model described in the documents in the file provides for the involvement of various data controllers, who intervene at different times and for the achievement of specific purposes. A central role is attributed to the GP called to carry out the patient enrollment phase and that of monitoring the individual patient regarding adherence to the proposed care model.

This organizational model of care was promoted, at the regional level, with some resolutions of the Tuscany Region (see DGRT nos. 650/2016 and 930/2017), but each health company has started it operationally, on its own initiative in the territorial area of competence, since 2017, coordinating the activities of GPs and providing them with organizational indications on the procedures and timing of the proposed care model.

In this context, the Company has also created the models containing the information to be given to the interested parties, for

the processing of personal data carried out by the same in the context of the healthcare initiative, providing that the GPs submit them to the patients to be enrolled.

The preliminary activity carried out by the Office concerned the activities carried out by the Company in the context of the treatments carried out through the implementation of the assistance model described above. From what emerged in the preliminary investigation, in an initial phase, the Healthcare Company, in carrying out the aforementioned coordination activities, did not process the personal data of patients who adhered to the aforementioned initiative healthcare model. From the beginning of 2018 and until September of the same year, due to the change in the methods of carrying out the activities connected to the implementation of this assistance model, the Company, on the basis of the consent of the interested party, instead processed personal data of patients enrolled as data controller for the purposes of monitoring, evaluation and quality of the assistance provided through the "initiative health care model" (cf. Disclosure model in documents).

Following the preliminary investigation carried out by the Office and the critical issues that emerged, the Company declared that, in order to achieve the aforementioned purposes, it will in the future only use aggregated and anonymous patient information that will be provided to it by GPs.

Having taken note of what is represented by the Company in the documentation in the deeds and in the defense briefs, it is noted that:

1. at the time of the inspection, the Company had not yet adopted, for all the treatments implemented by the same, the register of treatment activities envisaged by art. 30 of the Regulation, which was only adopted on 30 November 2018. Keeping the register is an essential element for the governance of the treatments and for the effective identification of those at greater risk. The Company was required to adopt the aforementioned register on the date of full application of the Regulation (May 25, 2018), as the derogation from register keeping envisaged by the Regulation does not operate in the presence of even just one of the elements indicated by art. 30, par. 5 (processing that presents a risk to the rights and freedoms of the interested party, non-occasional processing, processing that includes particular categories of data pursuant to article 9 or data relating to criminal convictions and offences), undoubtedly present in the present case. In this regard, it should also be borne in mind that the provisions of the Regulation were already in force on 25 May 2016 and that the two years elapsed before their full application should have been used by the data controllers precisely to adapt the treatments to the provisions of the Regulation;

2. the designation of ESTAR as data controller, carried out with a deed of 3 October 2016 with reference to the complexity of

the treatments carried out by this body on behalf of the Company, was found to be unsuitable with respect to the provisions of art. 28 of the Regulation but also to what is indicated in the art. 29 of the Code, in force at the time of the adoption of the appointment. In fact, the deed does not analytically indicate the tasks assigned to ESTAR in relation to the multiple treatments carried out by the Body, including those relating to self-initiated medicine (treatment of the personal data of patients present in the Excel files compiled by the referring district doctors for provincial areas, consolidation of this information, insertion of the same in a company data warehouse and creation of a data mart relating to the progress of the enrollment process by pathology and by doctor, which allowed the Company to carry out the aforementioned prevalence calculation) and, consequently, does not include specific instructions, in relation to the multiplicity of treatments carried out by ESTAR on behalf of the Healthcare Company (art. 29 of the Code, in force at the time of designation and art. 28 of the Regulation, in force at the time of the inspection assessment). The Company has taken steps to renew the designation of ESTAR as data processor with deed dated 27 December 2018;

3. with reference to the procedure, adopted starting from 2018, for sending the name data of patients enrolled by GPs to the Company, the same has not implemented adequate technical and organizational measures to guarantee a proportionate level of security at risk. The methods described above, ascertained during the inspection, (GPs save the Excel table on their own removable support (pen drive), delivery of the support to the district doctor, saving the file on the district doctor's PC and sending of the same - attached to an e-mail - to the referring district doctor for the provincial area, subsequent sending by the latter to ESTAR of the files received from all the district doctors, attaching them - in zip format with password for the opening of an e-mail message) do not, in fact, meet the security principles and criteria described in articles 5, par. 2, lit. f) and 32 of the Regulation. These treatment methods highlight the absence of an assessment of the risks of the treatment that should have been carried out in the context of the impact assessment which, on the other hand, does not appear to have been carried out;

4. the information model called "European regulation for the protection of natural persons with regard to the processing of personal data (n. 2016/679 GDPR) - Information pursuant to articles 13 and 14 of the Regulations" created by the Company, in its capacity as data controller for the purposes of monitoring, evaluation and quality of the assistance provided through the "Initiative healthcare model", and provided to GPs so that it was made to patients at the time of enrollment is missing some of the essential elements provided for by the legislation in force at the time of enrollment, such as: the retention period of personal data, the rights recognized by the Regulation to the interested parties, the right to lodge a complaint with the

Supervisory authority and the contact details of the controllers and the data protection officer. Furthermore, the aforementioned disclosure model did not provide clear indications regarding the treatment carried out by the Regional Health Agency "for purposes of monitoring and assessing the quality of assistance", with specific reference to the indication of the legal basis of the treatment. Although these models were prepared by the Company at a time prior to the date of application of the Regulation, they refer to a collection of data that took place during the period of application of the European legislation, which, moreover, is referred to in the header of the model. It should also be noted that these models are, in any case, also devoid of some of the essential elements that were already envisaged by the previous regulation (Article 13 of the Code) such as: the rights granted to the interested parties and precise indications regarding the role of the Regional Agency of healthcare. It should also be noted that the aforesaid model did not make any reference to other sources (e.g. the Internet sites of the various data controllers involved) for the acquisition of the missing information;

5. in light of the nature of the data processed and the number of interested parties, the treatment carried out by the Company in 2018, with reference to initiative healthcare, falls within the cases for which the owner cannot ignore an impact assessment on the protection some data. In this regard, however, it was ascertained that the Company had not carried out the required impact assessment pursuant to art. 35 of the Regulation. In this regard, it should be noted that, although the treatments began before the full application of the Regulation, the impact assessment was in any case necessary as they were also carried out during the period of full application of the Regulation. As shown above, some obvious shortcomings relating to the adoption of adequate security measures could have been avoided if the risk of the treatment had been adequately assessed. In this regard, it is noted that in the future the transmission of data to the Company by GPs will concern exclusively anonymous information.

With specific reference to the processing of personal data carried out in the context of the c.d. of initiative medicine, finally, it should be noted that the Guarantor recently in an opinion given to the Council of State represented that these models are often linked to a profiling of the patients (so-called "stratification" activity) which requires an adequate basis legal entity that has the characteristics required by the European Regulation (art. 6, par. 3) (Opinion to the Council of State on the new ways of allocating the health fund among the regions proposed by the Ministry of Health and based on population stratification - 5 March 2020 , web doc n. 9304455).

Lastly, the Guarantor also gave his opinion on a bill of the Autonomous Province of Trento which also contained provisions on

initiative medicine (opinion of 8 May 2020, web doc n. 9344635). In this regard, the Authority highlighted the need to proceed with a revision of the regulatory provisions, in order to take into account the principles of lawfulness, correctness, purpose limitation, minimization and safety of the Regulation, as they are united, without the necessary distinctions , treatments carried out for statistical purposes, administrative and treatment purposes. The Guarantor then recalled the specific constraints, in terms of data protection and transparency, which must be respected in the event that the medicine of initiative is based on the profiling of the patients through the use of an algorithm, referring to what was recently represented, in this regard, by the Council of State (Cons. St., section VI, 13 December 2019, n. 8472). In this context it has been highlighted that the collection and processing of health data, in order to create, with reference to specific pathologies, a health risk profile of the data subject constitutes an independent treatment with respect to the main one aimed at the care of the patient , which must therefore be carried out on the basis of the data subject's consent, as automated processing is not strictly necessary for the data subject's treatment purposes (articles 9, paragraph 2, letter h) and 22 of the Regulation). These considerations were also reaffirmed in the opinion issued by the Authority on a draft regulation relating to the implementing provisions of the aforementioned provincial law for initiative medicine in the Trentino provincial health service (opinion of 1 October 2020).

4. Conclusions.

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

For these reasons, the unlawfulness of the processing of personal data carried out by the Local Health Unit of South East Tuscany is noted, in the terms set out in the justification, for violation of articles 5, par. 2, lit. f), 13, 14, 28, 30, 32, 35 of the Regulation.

In this context, considering, in any case, that the conduct has exhausted its effects, given that the Company has declared that it has coordinated the modification of the models containing the information to be provided to the interested parties pursuant to

articles 13 and 14 of the Regulations, to have renewed the designation of ESTAR as responsible for the treatments carried out by the Body on behalf of the Company, which in the future - for the initiative health model - only anonymous information will be transmitted to the Company by GPs and that the register of treatments carried out by the Company has been adopted, the conditions for the adoption of the corrective measures pursuant to art. 58, par. 2, of the Regulation.

5. 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. f), 13, 14, 28, 30, 32, 35 of the Regulation, caused by the conduct put in place by the South East Tuscany Local Health Authority, is subject to the application of the administrative fine pursuant, respectively, to art. . 83, par.5, lett. b) and par. 4, lit. a) of the Regulation.

In the present case - also considering the reference contained in the art. 166, paragraph 2, of the Code – the violation of the aforementioned provisions is subject to the application of the same pecuniary administrative sanction provided for by art. 83, par. 5 of the GDPR, which therefore applies to the present case.

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 Board [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 it is observed that:

- the Authority has received only one report from a GP regarding the processing of data carried out by the Healthcare Company with reference to the initiative healthcare model and no thefts, loss of data or unlawful treatment by the various subjects have been reported involved in the processing of data (Article 83, paragraph 2, letter a) and h) of the Regulation);

- the data processing carried out by the Company, through the initiative health model, concerns data suitable for detecting

information on the health of numerous interested parties, or all the patients of the same Company (art. 4, paragraph 1, no. 15 of the Regulation and article 83, paragraph 2, letters a) and g) of the Regulation);

- the Company, also as a result of a failure to assess the risk, had not adopted adequate security measures in relation to the data processing methods carried out by the doctors and had not adopted (at the time of the inspection) nor the register of processing activities, fulfilments which are an expression of the principle of accountability established by the Regulation (Article 5, paragraph 2 of the Regulation);

- the Company has demonstrated a high degree of cooperation, providing for the modification of the model of self-initiated medicine, providing, for the future, that only anonymous information is transmitted to it and taking an active part in the creation of a new model relating to information to be provided to data subjects (Article 83, paragraph 2, letters c), d) and f) of the Regulation);

- the institutional process for the integration into the regional legislation of a complete regulation of the healthcare model of initiative has started.

Based on the aforementioned elements, evaluated as a whole, also taking into account the phase of first application of the sanctioning provisions pursuant to art. 22, paragraph 13, of Legislative Decree lgs. 10/08/2018, no. 101, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 4, lit. a) and par. 5, letter. b) of the Regulation, to the extent of 100,000.00 (one hundred thousand) euros for the violation of articles 13 and 28 of the Regulation as a pecuniary administrative sanction withheld, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive. In quantifying the fine, the Guarantor took into particular consideration the fact that the violations are connected to a treatment started shortly before the definitive application of the Regulation.

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 potential number of interested parties and 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 unlawfulness of the processing of personal data carried out by the Local Health Unit of South East Tuscany, for

the violation of the articles 5, par. 2, lit. f), 13, 14, 28, 30, 32, 35 of the Regulation in the terms indicated in the justification.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the South East Tuscany Local Health Authority, with registered office in Arezzo (AR), Via Curtatone, 54 - C.F./P. 02236310518, in the person of the pro-tempore legal representative, to pay the sum of 100,000.00 (one hundred thousand) euros as an administrative fine for the violations indicated in this provision, according to the procedures indicated in the annex, within 30 days of notification in 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 fine imposed.

ENJOYS

to the aforementioned Company, to pay the sum of Euro 100,000.00 (one hundred thousand), according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of adopting the consequent executive deeds pursuant to art. 27 of the law n. 689/1981. In this regard, it is recalled that the offender retains the right to settle the dispute by paying - always according to the methods indicated in the annex - an amount equal to half of the fine imposed, within 30 days from the date of notification of this provision, pursuant to art. 166, paragraph 8, of the Code (see also art. 10, paragraph 3, of Legislative Decree no. 150 of 09/01/2011);

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, 17 December 2020

PRESIDENT

Station

THE SPEAKER

Cerrina Feroni

THE SECRETARY GENERAL

Matthew