SEE NEWSLETTER OF 11 MAY 2022

[doc. web n. 9768363]

Injunction order against the Perugia hospital - 7 April 2022

Record of measures

n. 134 of 7 April 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

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

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

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

GIVEN the documentation in the deeds;

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

SPEAKER Attorney Guido Scorza;

WHEREAS

1. Introduction.

As part of a cycle of inspection activities, concerning the main functions of some of the applications for the acquisition and management of reports of offenses most widely used by public and private employers within the framework of the regulations on reporting unlawful conduct (so-called whistleblowing), which provides for specific guarantees to protect the identity of the reporting party, specific investigations were carried out against the Perugia hospital (hereinafter the "Company"; see minutes of the operations carried out in the twentieth century), and by ISWEB S.p.A. (hereinafter, the "Company"), which supplies and manages on behalf of numerous customers, including the Company, the application used for the acquisition and management of reports of illegal conduct and, for this purpose, is identified as data processor (see minutes of operations carried out in the 20th century).

This also in light of the provisions, with regard to the initiative inspection activity carried out by the Guarantor's Office, with resolutions of 12 September 2019, doc. web n. 9147297, of 6 February 2020, doc. web n. 9269607, and of 1 October 2020, doc. web n. 9468750.

2. The preliminary activity.

At the outcome of the investigation, given the particular complexity of the technological profiles that emerged during the investigation (see technical report of the XXth), it emerged that:

- "the Company, with Resolution of the General Manager of 22 December 2016, no. 2341, adopted, pursuant to l. 190/2012, the "Company regulation for the protection of the employee who reports offenses (whistleblower)" which, in art. 2, in specifying the subjective scope of application of the same, clarifies that the subjects who can report are: employees, collaborators, consultants, trainees, trainees, volunteer visitors and all subjects who, for any reason, carry out activities within the 'agency";
- "The submission of a report can be made: (a) in paper form, by means of the postal service, by sending the form published on the company website to the Head of Corruption Prevention and Transparency (RPCT); (b) verbally directly to the RPCT; (c) in computer mode, using a dedicated web application ";
- "The Company uses a web application managed and provided, in cloud mode, by the company Internet Solutions S.r.l. (now ISWEB S.p.a.) ", whose relationship was governed pursuant to art. 28 of the Regulation (see the resolution of the General Manager of 23 September 2016, n.1678, with which the purchase of the aforementioned web application was approved, as well as the deed of designation as data processor of the company ISWEB S.p.a. of the XX , att. 13 and 16 to the minutes of the XX; see also annex 5 to the minutes of the XX);

- "the processing relating to the acquisition and management of reports of illegal conduct (so-called whistleblowing) [...] is not described in the treatment register";

- "the Company has not prepared specific information on this subject, although a general information on the processing of personal data of employees is included in the individual employment contracts" (see annexes 18 and 19 to the minutes of the 20th).

- "the web application, although exposed on the public network at the address" https://whistleblowing.ospedale.perugia.it/ ", can only be reached from workstations certified to the company network";

- "The Company has made an operating manual available on the company website that illustrates how to send a report through the web application in question. In particular, a first phase of "Registration in the system" is envisaged to be carried out at the time of the first report which involves the insertion of some identification and contact data of the reporting party, as well as the qualification and the place of employment. Following this registration, the web application shows the reporting party the so-called "Whistleblower code" and, at the same time, sends an email to the subject with the role of "person in charge of managing the registry of members". After this phase, it is possible to send a report using the “Make a report” function which requires the compilation of fields relating to the conduct subject to reporting and to the persons who have carried it out. Following the submission of the report, the web application shows the reporting party the so-called "Reporting code" that allows you to monitor the progress of the report, to integrate it and to exchange messages with the RPCT ";

- "following the submission of the report, the web application sends an email to the subject with the role of" responsible for the prevention of corruption "";

- "access to the public network takes place through new generation firewall systems, which make it possible to configure specific internet browsing rules, also based on the role and the different functions performed by employees or other subjects who have access to the company network [...] "these firewall systems store the navigation operations carried out in special log files, together with data that allow you to trace, even indirectly, the employees or other subjects who carried them out [...] no specific precautions have been envisaged in order not to register browsing operations on the web application for the acquisition and management of reports of illegal conduct ";

- the "internet browsing logs are stored in a virtual server connected to the firewall until the maximum size of the log file is reached (150 GB) [...] when this size is reached, the oldest records are overwritten by the most recent records "And" as part of

the backup procedures, these logs are kept for a further period that the Company reserves the right to communicate ";

- "the only person authorized to process reports of illegal conduct is the RPCT, a task that was carried out by Dr. [...] from 2013 to May 2, 2019, date from which the resignation presented by the same became effective ";

- following the resignation of the RPCT, "the two authentication credentials (one for verifying the registry of the reporting persons and one for managing the reports) used by the same to access the application in question were delivered by the latter to the manager of the Office for the prevention of corruption, transparency and processing of personal data in a sealed envelope ";

- the aforementioned "authentication credentials are still active and that the e-mail address on which the web application sends the notifications of the registration of a reporting party and the receipt of a report is the one assigned to Dr. [...]" ;

- the Company "notified ANAC of the termination of Dr. [...], Administrative Director of the Company "; "The extraordinary nature of the situation in which the Company finds itself has not made it possible to identify the RPCT among the executives in service and that an exploratory activity has been launched aimed at identifying a subject, preferably external, suitable to cover this function which, to date , has not yet had a positive outcome ";

- "the aforementioned authentication credentials (one for verifying the registry of reporting persons and one for managing reports) have not yet been assigned to the new RPCT";

- "The Hospital has not carried out the impact assessment on this treatment pursuant to art. 35 of the Regulation ".

During the investigations carried out at the Company, the same declared (see minutes of the XX, pp. 3 et seq.) As follows:

- "the company markets a service based on open source software called" GlobalLeaks ", taking care of its installation, configuration (both during activation and during the contractual relationship) as well as the technical maintenance of the same. Currently, the service is provided through two dedicated servers on which two different versions of the "GlobalLeaks" software are installed: the first (version 2.60.113) in production since 2015 and in use by most customers will be progressively replaced by the second (version 3.10.8), more updated, currently in use by a more limited number of customers ";

- version 2.60.113 of the "GlobalLeaks" software, also in use by the Perugia hospital (see Annex 8 to the 20th minute) "takes into account the indications contained in the 2015 ANAC guidelines. in order to ensure the separation of the identifying data of the whistleblower from the content of the report, the whistleblowing application makes two distinct procedures available to whistleblowers: the first allows registration on the application with the release of the so-called "Reporting code", necessary for

sending a report, while the second allows the sending of a report with the release of the so-called "Report code", required to check the status of a report. The whistleblowing application provides a back-office interface through which registrations are validated by subjects with the profile of "registry administrator" (who verify that the subscriber is a subject entitled to send the report) and reports are managed by subjects with the profile of "whistleblower" "(see also Annex 8 to the minutes of the XXth);

- "the reports are fully accessible and manageable only after the validation of the reporting party's registration, even in cases where they have been previously transmitted. The application does not provide for the sending of notification messages to the e-mail address of the reporting party, as the latter has the ability to consult the status of the report through the so-called "Reporting code". Otherwise, the application provides for the sending of notification messages on the e-mail addresses of subjects with the profile of "registry administrator" and "notification administrator" ";

- "subjects with the profile of" whistleblower "(usually the RPCT) can have access to the identification data of the whistleblower after entering a specific reason that is recorded on the whistleblowing application and is also visible to the whistleblower during consultation the status of the report ";

- version 3.10.8 of the "GlobalLeaks" software, "contrary to the previous one which provided for two different forms for registering whistleblowers and sending reports, provides whistleblowers with a single form for submitting a report of unlawful conduct. As part of this procedure, a whistleblower can choose to remain anonymous or to enter data relating to his or her identity. Even in the case of an originally anonymous report, the whistleblower has the right to access the whistleblowing application through the so-called "Report code" - generated following the submission of the report - to check the status of the report and possibly to enter data relating to its identity ";

- "the whistleblowing application, also in order to guarantee an effective separation of the identifying data of the whistleblower from the content of the report, provides for a specific procedure to make the data relating to the whistleblower's identity visible to subjects with the profile of" reports ". In fact, it is possible to assign the profile of "identity guardian" to subjects operating under the authority of the data controller, to whom subjects with the "whistleblower" profile can request, after entering an appropriate motivation , access to data relating to the identity of the whistleblower. Subjects with the "identity guardian" profile do not have access to either the data relating to the identity of the whistleblower or the content of the report but can only view the reason associated with the request for access to the data relating to the identity of the whistleblower ";

- "Among the various customizations allowed by the whistleblowing application, it is possible: (1) the person with the"

whistleblower "profile can also send files to the whistleblower; (2) the subject with the profile of "reporting administrator" can independently carry out the export, cancellation, disabling of notifications and extension of the predefined deadline for "reporting expiration" (after which the data of the report are securely deleted); (3) the subject with the "tenant administrator" profile can, in configuring the so-called "Questionnaires" that define the structure of the reporting form, define rules to allow the visibility of a specific type of report to a specific subject with the profile of "reporting administrator" (eg a staff member assigned to the RPCT) ";

- "the security measures adopted to protect the data processed with the aid of the whistleblowing application" are described in specific documents provided by the Company (see Annexes 2 and 3 to the minutes of the XXth);
- "the" GlobalLeaks "software uses secure protocols for data transport (https) and encryption tools for data retention (content of reports and any attached documentation), also described in the document that describes the security measures of the application whistleblowing "(see attachment 2 to the minutes of the 20th);
- "The access and operations performed on the whistleblowing application by subjects with the profile of" registry administrator "and" reporting administrator "are to be tracked in special log files. With reference to accesses and operations carried out by whistleblowers, the whistleblowing application does not store, in the log files, the IP address of the device used by them ";
- "ISWEB has prepared an impact assessment on data protection relating to the processing of personal data carried out by the company and which it makes available to its customers" (see Annex 4 to the minutes of the XXth);
- the Perugia hospital has requested the Company to make the "changes necessary following the appointment of a new head of corruption prevention and transparency (RPCT)" (see correspondence, annex 6 to the minutes of the XXth) ;
- "the company has entrusted the company Seeweb S.r.l. with the hosting service of the IT systems that host, among others, the whistleblowing application, providing the contract and the" Description of services and GDPR Compliance "[...], documents which show the roles of the two companies in the processing of personal data "(see attachment 7 to the minutes of the 20th; see the act of appointment of Seeweb s.r.l., attached to the subsequent note of the 20th).

With a note of the twentieth, the Office, on the basis of the elements acquired, notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in art. 58, par. 2, of the Regulation, inviting the aforementioned data controller to produce defensive writings or documents to the Guarantor or to ask to be heard by the Authority (Article 166, paragraphs 6 and 7, of the Code; as well as Article 18, paragraph 1, of the Law No.

689 of November 24, 1981).

With the aforementioned note, the Office found that the Company has carried out processing of personal data of employees and other interested parties, through the use of the application for the acquisition and management of illegal reports, in a non-compliant manner. to the principles of "lawfulness, correctness and transparency" and without providing the interested parties with information relating to the processing, in violation of art. 5, par. 1, lett. a), 13 and 14 of the Regulations; in a manner that does not comply with the principles of "integrity and confidentiality", "data protection by design" and "data protection by default", in violation of Articles 5, par. 1, lett. f), and 25 of the Regulations; in the absence of appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the processing, in violation of art. 32 of the Regulation; not having reported in the treatment register the activities of acquisition and management of reports of illegal conduct, in violation of art. 30 of the Regulation; not having carried out an impact assessment on data protection, in violation of art. 35 of the Regulation.

With a note of the twentieth century, the Company sent its defense briefs, attaching the necessary documentation to prove the measures taken with regard to the treatments in progress against the generality of employees, and specifying, among other things, that:

- "at the time of carrying out the inspection activities [...] the Company had been hit by a judicial investigation which [...] has, in fact, upset the organizational structure within the Company, preventing it from carrying out accurately and timely many of its ordinary administrative activities [...] In this context, the Company has in any case carried out its main functions (first of all the protection of citizens' health) and has found itself, in spite of itself, forced to adopt, at times, some precarious solutions ";
- "This context, therefore, heavily influenced the issues that the Authority disputes in its minutes and it cannot be ignored as it was not an" ordinary "situation but one of the most important judicial inquiries of the last 30 years of the Umbria Region with a "zeroing" of the executive class and the top positions of this Company ";
- "As you know, the Covid-19 pandemic has hit our country (and the rest of the world) since February 2020 [...] The Perugia Hospital is the most important hospital in the Umbria Region and most of the Covid sufferers. […] This health emergency situation has heavily involved the entire organization of the hospital, both health and administrative, with internal organizational difficulties and an increase in costs and expenses which cannot be ignored ";
- "no report [... of illegal conduct] has ever reached the system appointed by the Company to send and receive said reports.

This aspect cannot be considered secondary since at the time of the inspection, but also subsequently, no processing of personal data or of confidential information has materialized and therefore, from the point of view of substantial protection, no illegal treatment or non-compliant treatment can be considered carried out ";

- with regard to the "failure to fulfill the obligation to disclose information to the interested parties", it is specified that "in the section dedicated to this there was, already at the time of the inspection, an introductory part specifying the function of the report and the guaranteed anonymity of the whistleblower "subsequently" in the aforementioned section [a structured information notice has been inserted which can be obtained from the link https://www.ospedale.perugia.it/pagine/segnalazione-illeciti-whistleblowing [... and it has also been posted] in the workplace and / or on the company bulletin board ";

- "the processing register was integrated with the section dedicated to whistleblowing";

- “the firewall system in place at the time, while recording the user's IP address and credentials, did not detect the activities that the user could have carried out after accessing the dedicated web page https: //whistleblowing.ospedale.perugia. it /. Furthermore, access to the consultation of the logs could only be carried out by the System Administrator (which, however, never occurred). It should be noted that following the inspection by this Authority, the Company made a substantial change: access to the web page https://whistlerblowing.ospedale.perugia.it/ was excluded from the registration of the logs and therefore is not possible to trace any access data ";

- “the authentication credentials of the resigning RPCT […] remained active as the resignation of the aforementioned Responsible party was not formally accepted and acknowledged until the appointment of the subsequent RPCT identified in the person of the Administrative Director”;

- "at the time of the decision on the need to adopt an impact assessment on the processing of personal data relating to possible reports of illegal conduct, it was decided to consider sufficient, at that moment, the DPIA - Data Protection Impact Assessment carried out by the software supplier management of the "Isweb" whistleblowing program ”; during the investigation, the Company "decided to adopt a specific DPIA".

The hearing requested by the Company was also held on the 20th, pursuant to art. 166, paragraph 6, of the Code, on the occasion of which the Company confirmed what was already stated in the defense briefs, and it was represented, among other things, that:

- "from January 1, 2021 [...] various initiatives were launched also aimed at improving the governance of corporate processes relating to anti-corruption and the protection of personal data";

- "there has been no violation of personal data as no report of illegal conduct has been acquired and processed through the whistleblowing application subject to the inspections";

- "the Company is actively participating in the drafting of a code of conduct for the sector, promoted by ALTEMS of the Catholic University of the Sacred Heart" and has carried out numerous training courses and "further training courses for employees are planned, within which specific training sessions on the use of the whistleblowing application are envisaged ".

3. Outcome of the preliminary investigation. Applicable legislation: the rules on the protection of employees who report offenses and the rules on the protection of personal data

The adoption of systems for reporting offenses (so-called whistleblowing) for its implications regarding the protection of personal data has long been under the attention of the Supervisory Authorities (Report of the Guarantor to Parliament and the Government available at www.garanteprivacy.it , web doc. 1693019; see, also, Group pursuant to art. 29, "Opinion 1/2006 on the application of EU data protection legislation to internal procedures for reporting irregularities concerning bookkeeping, internal accounting controls, auditing, the fight against corruption, banking and financial crime ", adopted on 1 February 2006). In recent years, there have been numerous interventions also of a general nature on the subject (see provision of 4 December 2019, no. 215, web doc. No. 9215763, opinion of the Guarantor on the outline of "Guidelines on of the authors of reports of crimes or irregularities of which they have become aware due to an employment relationship, pursuant to art. 54-bis of Legislative Decree 165/2001 (so-called whistleblowing) "of ANAC) and decisions on individual cases (see provisions no. 235 of 10 June 2021, web doc. 9685922, and 236, web doc. 9685947; see newsletter no. 480 of 2 August 2021, web doc. no. . 9687860, but already provision. 23 January 2020, n. 17, web doc. N. 9269618; newsletter n. 462 of 18 February 2020, web doc. N. 9266789); lastly, the Guarantor during a hearing in Parliament recalled that in exercising the delegation for the transposition of Directive (EU) 2019/1937 (concerning the protection of persons who report violations of Union law) it is necessary " to achieve an appropriate balance between the need for confidentiality of the report - functional to the protection of the whistleblower -, the need to ascertain the offenses and the right of defense and to cross-examination of the reported person. The protection of personal data is, of course, a determining factor for the balance between these instances and for this reason it is appropriate to involve the Guarantor during the exercise of the delegation "(see, Hearing of the Guarantor for the

protection of personal data on the legislative decree 2021 European Delegation - Senate of the Republic - 14th Parliamentary Commission of the European Union, 8 March 2022, web doc. no. 9751458).

The matter was initially regulated within the framework of the general rules on the organization of work employed by public administrations (see Article 54-bis of Legislative Decree no. 165 of March 30, 2001, introduced by Article 1, paragraph 51, of Law No. 190/2012, containing provisions for the prevention and repression of corruption and illegality in the public administration). Subsequently, the regulatory framework was defined with l. 30 November 2017, n. 179 (in the Official Gazette of 14 December 2017, no. 291) containing "Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship" which amended the relative regulations to the "protection of public employees who report offenses" (see new version of art. 54-bis of legislative decree no. 165/2001 and art. 1, paragraph 2, of law no. 179/2017) and introduced a new discipline on whistleblowing referred to private subjects, integrating the legislation on "administrative liability of legal persons, companies and associations, including those without legal personality" (see Article 2, Law No. 179/2017 which added the paragraph 2-bis of Article 6 of Legislative Decree no. 231 of 8 June 2001).

The aforementioned regulatory framework - which updated the previous discipline under various profiles, from the sanctioning framework (see Article 54-bis, paragraph 6, cit.), To the specific safeguards for the person concerned, such as reintegration into the workplace in the event of dismissal "due to reporting" and the nullity of any "discriminatory or retaliatory acts" (Article 54-bis, paragraphs 7 and 8, cit.) -, provides, more generally, measures aimed at protecting disclosure the identity of the whistleblower, in order to prevent the adoption of discriminatory measures against the same. In this context, in fact, "the identity of the whistleblower cannot be revealed" (art. 54-bis, paragraph 3, cit.), With some reconciliation (see art. 54-bis, paragraphs 3 and 9, cit. , in relation to the criminal, accounting or disciplinary proceedings that may result from the report or "in cases in which the criminal responsibility of the reporting party is ascertained, even with a first degree sentence, for the crimes of slander or defamation or in any case for crimes committed with the [report or if it is ascertained] his civil liability, for the same reason, in cases of willful misconduct or gross negligence "). The report is also removed from the access provided for by articles 22 and following of the law of 7 August 1990, n. 241, and subsequent amendments (Article 54-bis, paragraph 4, cit.).

Given the art. 54-bis, paragraph 5, which provides for the adoption by ANAC, after consulting the Guarantor, of specific guidelines relating to the procedures for the presentation and management of reports, the Guarantor, with provision of 4

December 2019 (doc. web n.9215763), has given its opinion on the outline of guidelines, confirming that the sector regulations on whistleblowing must be coordinated, in application, with the legislation on the protection of personal data. Therefore, the subjects obliged to comply with the aforementioned provisions must process the data necessary for the acquisition and management of reports also in compliance with the personal data protection regulations.

In this context, the processing of personal data carried out by the obliged subjects can be considered necessary to fulfill a legal obligation to which the data controller is subject (articles 6, paragraph 1, letter c), 9, par. 2, lett. b), and 10 of the Regulation). For these reasons, the aforementioned sector regulations, which involve the processing of employee data reporting offenses, must be considered as one of the "most specific rules to ensure the protection of rights and freedoms with regard to the processing of personal data of employees. in the context of employment relationships ”provided for by art. 88, par. 1, of the Regulation (see, most recently, provisions no. 235 of 10 June 2021, web document no. 9685922, and no. 236 web doc. No. 9685947; see newsletter no. 480 of 2 August 2021 , web doc. n. 9687860; but see already provision of 4 December 2019, n. 215, web doc. n. 9215763, opinion of the Guarantor on the outline of "Guidelines for the protection of the authors of reports of crimes or irregularities of which they have become aware due to an employment relationship, pursuant to Article 54-bis of Legislative Decree 165/2001 (so-called whistleblowing) "of ANAC).

More generally, the data controller is in any case required to comply with the principles of data protection (Article 5 of the Regulation) and the data must also be "processed in such a way as to guarantee adequate security" of the same, "including the protection , by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage "(articles 5, paragraph 1, letter f), of the Regulations).

The owner, in the context of the necessary identification of the technical and organizational measures suitable to guarantee a level of security adequate to the specific risks deriving from the treatments in question (articles 24, 25 and 32 of the Regulation), must define his own model for managing the reports in accordance with the principles of "data protection by design" and "protection by default", also taking into account the observations presented in this regard by the data protection officer (DPO).

3.1. Failure to fulfill the obligation to disclose information to interested parties.

With regard to the principle of "lawfulness, correctness and transparency", the owner is obliged to provide in advance to the entire audience of possible interested parties specific information on the processing of personal data and must adopt

"appropriate measures to provide the interested party with all the information referred to in articles 13 and 14 […] "of the Regulations (article 12 of the Regulations).

However, in the course of the investigation, the Company stated that it had not made specific prior information in relation to the processing resulting from the acquisition of reports of alleged offenses, nor the information on the processing required by Articles 13 and 14 of the Regulations are otherwise provided by the Company, not being, for example, included in the organizational act adopted by the owner for the management of reports, or published in a specific section of the computer application used for the acquisition and management of reports, or, again, in individual employment contracts.

Nor can the circumstance represented in the defense briefs be considered sufficient on the basis of which "in the section dedicated to this there was, already at the time of the inspection, an introductory part specifying the function of the report and guaranteed anonymity of the reporting party ". These initiatives cannot replace the information that the data controller must provide, before starting the processing, to the interested parties regarding the essential characteristics of the same (see Judgment of the European Court of Human Rights of 5 September 2017 - Appeal no. 61496 / 08 - Barbulescu case vs Romania, spec. N. 140).

It is acknowledged that in the course of the procedure, the Company has prepared an information notice dedicated to the processing connected to the acquisition and management of reports of illegal conduct, as documented on the occasion of the defense briefs (see Annex A to the note of XX).

For these reasons, until the adoption of the new information document relating to the treatments in question, made available to interested parties, the Company did not operate in accordance with the principle of correctness and transparency and therefore in violation of Articles 5, par. 1, lett. a), 13 and 14 of the Regulation.

3.2. Failure to indicate treatments for whistleblowing purposes in the register of processing activities

Art. 30 of the Regulation provides, among the main obligations of the data controller, to keep the register of processing activities, which must be in written form, including electronic, and must be shown upon request to the Guarantor. Keeping the register, which must contain the main information relating to the processing operations carried out, is functional to compliance with the principle of "accountability" of the owner (Article 5, paragraph 2, of the Regulation), as it constitutes a suitable tool for provide an updated picture of the treatments in place within the owner's organization. This is particularly relevant with regard to risk assessment and analysis activities, thus constituting a preliminary fulfillment with respect to such activities.

The Regulation identifies in detail the information that must be contained in the register of the data controller's processing activities, including the purposes of the processing (Article 30, paragraph 1, letter b)) also, where appropriate, with the indication of its legal basis. In the present case, however, as verified during the inspection and confirmed by the Company, the processing of personal data carried out for the purpose of acquiring and managing reports of illegal conduct (so-called whistleblowing) were not registered in the register of activities of treatment.

It is acknowledged that during the procedure the Company has supplemented the aforementioned register with reference to the processing connected to the acquisition and management of reports of illegal conduct, as documented on the occasion of the defense briefs (see Annex B to the note of the XX).

For these reasons, it must be considered that, until the register of processing activities is updated, the Company has not fulfilled the aforementioned obligation, in violation of art. 30 of the Regulation.

3.3. Tracking access to the application.

During the investigation it was found that the application for the acquisition and management of reports of illegal conduct, which can be reached at the address "https://whistleblowing.ospedale.perugia.it/", is accessible only from work attested to the company network and that "access to the public network [from such workstations] takes place through new generation firewall systems" (see minutes of the 20th, pp. 5 and 6). Furthermore, it emerged that "these firewall systems memorize the navigation operations carried out in special log files, together with data that make it possible to trace even indirectly the employees or other subjects who carried out them". Moreover, it emerged that "no specific precautions have been envisaged in order not to register browsing operations on the web application for the acquisition and management of reports of illegal conduct" (see minutes of the XXth, p. 6).

In this regard, the Company specified that "these internet browsing logs are stored in a virtual server connected to the firewall until the maximum size of the log file (150 GB) is reached and that, upon reaching this size, the records oldest are overwritten by the most recent records ". Furthermore, "as part of the backup procedures, these logs are kept for a further period" (see minutes of the XXth, p. 6). Subsequently, the Company announced that it had "expanded the storage space to ensure the saving of the last three complete months" (see note of the XXth).

As is clear from the documentation acquired during the inspections, the logs generated by the aforementioned firewall devices contain, among others, the IP address of the workstation used to connect to the application in question and the username of

the person who made this connection. .

Having said this, it is noted that the recording and storage, in the logs of the firewall devices, of the information relating to the connections to the application in question allows the traceability of the subjects who use this application, including the reporting persons. This, also considering the small number of connections to the application in question, renders the other measures adopted to protect the confidentiality of the identity of the reporting parties ineffective. For these reasons, the registration and storage, within the logs of the firewall devices, of information directly identifying the users of the application in question does not comply with the provisions of art. 5, par. 1, lett. f), and art. 32 of the Regulation which establishes that the data controller must implement measures to "ensure on a permanent basis the confidentiality, integrity, availability and resilience of the processing systems and services" (paragraph 1, letter b)) and that "in assessing the adequate level of security, particular account is taken of the risks presented by the processing that derive in particular from the destruction, loss, modification, unauthorized disclosure or access, in an accidental or illegal way , to personal data transmitted, stored or otherwise processed "(par. 2).

Furthermore, it is noted that, based on the principle of "data protection by design" (Article 25, paragraph 1, of the Regulation), the data controller must adopt adequate technical and organizational measures to implement the principles of protection of data (Article 5 of the Regulation) and must integrate in the processing the necessary guarantees to meet the requirements of the Regulation and protect the rights and freedoms of the data subjects. This obligation also extends to treatments carried out by means of a data controller. In fact, the processing operations carried out by a manager should be regularly examined and evaluated by the owner to ensure that they continue to comply with the principles and allow the owner to fulfill the obligations established by the Regulation (see "Guidelines 4/2019 on article 25 Data protection by design and by default ", adopted on 20 October 2020 by the European Data Protection Board, spec. Points 7 and 39). Therefore, the failure to adopt the aforementioned measures - aimed at implementing the principles of data protection and integrating the necessary guarantees in the processing in order to meet the requirements of the Regulation - is also in contrast with the principle of "data protection by design "Pursuant to art. 25, par. 1, of the Regulation.

In this framework, moreover, the data controller, in addition to respecting the principle of "data protection by design" (Article 25, paragraph 1, of the Regulation) - adopting technical and organizational measures adequate to implement the protection principles of the data (art. 5 of the Regulation) and integrating in the processing the necessary guarantees to meet the

requirements of the Regulation and protect the rights and freedoms of the data subjects - must also, in compliance with the principle of "data protection by default" (art . 25, par. 2, of the Regulation), make choices that ensure that, by default, only the processing strictly necessary to achieve a specific and lawful purpose is carried out. This therefore implies that, by default, the data controller must not collect personal data that are not necessary for the specific purpose of the processing (see "Guidelines 4/2019 on article 25 Data protection by design and by setting default ", adopted on 20 October 2020 by the European Data Protection Board, spec. points 42, 44 and 49).

As recently highlighted by the Guarantor, precisely in the context of the treatments carried out through applications for the acquisition and management of unlawful reports, the data controller, even when using products or services made by third parties, must perform, also making use of the support of the data protection officer where appointed, an assessment of the risks and make sure that the functions that do not have a legal basis, are not compatible with the purposes of the processing, or are in contrast with specific sector regulations provided for by the law, are disabled , in particular, the regulations on whistleblowing (see provision 10 June 2021, no. 235, web doc. no. 9685922, spec. par. 3.2, and the provisions referred to therein), but also the national regulations regulate the conditions for the use of technological tools in the workplace (under this last profile, with regard to operations for tracing connections to Inter net by employees, v. most recently prov. May 13, 2021, n. 190, doc. web n. 9669974).

In this regard, for the purposes of the overall assessment of compliance with the processing security obligations, the information highlighted by the Company regarding the fact that "while registering the IP address and user credentials" the firewall device "did not detect the activities that the same could have carried out after accessing the dedicated web page https://whistleblowing.ospedale.perugia.it/ "and that" access to the consultation of the logs could only be carried out by the System Administrator (circumstance however, never happened) "(see note of the XX).

It is acknowledged that, during the investigation, the Company stated that "access to the web page https://whistlerblowing.ospedale.perugia.it/ has been excluded from the registration of the logs and therefore it is not possible to trace no access data "(see note of XX).

For these reasons, it is believed that the registration and storage, within the logs of the firewall devices, of information relating to the connections to the application in question by users - even if only relating to the mere access and consultation of the web pages of the application - was put in place, up to the moment in which the owner took steps to adopt the aforementioned

measures to protect the interested parties, in violation of articles 5, par. 1, lett. f), 25 and 32 of the Regulations.

3.4. Unsuitability of the methods of managing the authentication credentials used by the RPCT.

During the investigation, the Company stated that "the only person authorized to process reports of illegal conduct is the RPCT, a task that was carried out by Dr. [...] from 2013 to May 2, 2019, effective date of which the resignation presented by the same became effective "(cf. minutes of the XXth, p. 6).

Following the resignation of the RPCT, "the two authentication credentials (one for verifying the reporting details and one for managing reports)" used by the same to access the application in question were delivered by the latter to the manager of the Office for the prevention of corruption, transparency and processing of personal data in a sealed envelope. Furthermore, the Company specified that the aforementioned authentication credentials, not yet assigned to the new RPCT, had remained active and that "the e-mail box on which the web application sends [goes] the notifications of the registration of a reporting and the receipt of a report [… was] the one assigned to Dr. […] "(see minutes of the XXth, p. 6).

Taking into account the nature, object, context and purposes of the processing, which involves the acquisition and management of reports of unlawful conduct, which may contain personal data - also belonging to particular categories or relating to criminal convictions. and offenses (articles 9, par. 1, and 10 of the Regulation) - referring or attributable to the reporting party, the person reported or third parties in any case involved in the reported facts, it is believed that the aforementioned methods of managing the authentication credentials for access the application in question are not adequate in terms of safety.

In acknowledging that, following the inspections, the Company first asked the Company to suspend the sending of notification e-mails from the application in question and, subsequently, asked to configure the address e-mail address of the new RPCT as the recipient of the notification e-mails relating to the registration events of a whistleblower and the receipt of a report (see annex 6 minutes of the XXth), it is noted, however, that the failure to deactivate the aforementioned authentication credentials (username and password) - following the loss of the qualities that allowed the resigning RPCT, to whom these credentials were attributed, to access the personal data processed within the application - has entailed a high and unjustified risk for rights and freedoms of the data subjects, in consideration of the serious consequences that would arise from any unauthorized access to the data contained in reports of conduct unlawful acts that could have been received in the period from 2 May 2019 (date from which the resignation of the RPCT became effective) to 2 July 2019 (date on which the Company, with the support of the

Company, reconfigured the application to allow its use by the new RPCT).

It is noted, in fact, that when - as in the case in question - the conditions that allow a subject to access a personal data processing system no longer exist and the authentication credentials used by the same are not promptly deactivated (or in any case to make them unusable by changing the relative passwords), situations may arise that make it possible for an unauthorized person to operate, in the absence of a specific will of the data controller, within this processing system. This circumstance is particularly relevant taking into account the particular confidentiality regime for the identity of the reporting party required by law.

For these reasons, while taking into account the clarifications made by the Company during the defense briefs (with specific regard to the fact that "the authentication credentials of the resigning RPCT [...] remained active as the resignation of the aforementioned Responsible party was not formally accepted and implemented up to the appointment of the next RPCT identified in the person of the Administrative Director "), the aforementioned methods adopted for managing the authentication credentials for access to the application in question do not comply with the provisions of art. 5, par. 1, lett. f), and art. 32 of the Regulation which establishes that the data controller must implement measures to "ensure on a permanent basis the confidentiality, integrity, availability and resilience of the processing systems and services" (paragraph 1, letter b)) and that in "assessing the adequate level of security, special account is taken of the risks presented by the processing that derive in particular from the destruction, loss, modification, unauthorized disclosure or access, in an accidental or illegal way , to personal data transmitted, stored or otherwise processed "(par. 2).

3.5. Failure to perform a data protection impact assessment.

As is clear from the preliminary evidence in the documents, the processing of the personal data of the data subjects was carried out in the absence of a preliminary impact assessment on data protection (see minutes of the XXth, p. 7).

In this regard, it should be noted, however, that, taking into account the indications provided also at European level, the processing of personal data through the systems for the acquisition and management of reports presents specific risks for the rights and freedoms of the data subjects, also considering the particular sensitivity of the information potentially processed, the "vulnerability" of the data subjects in the working context, as well as the specific confidentiality regime for the identity of the whistleblower provided for by the sector regulations (see articles 35 and 88 par. 2 of the Regulation; impact assessment on data protection as well as the criteria for establishing whether a treatment "may present a high risk" pursuant to Regulation

2016/679, WP 248 of 4 April 2017; see, most recently, provision of 10 June 2021, no. . 235, web doc. N. 9685922, but already provided on 4 December 2019, web doc. N. 9215763, with which the Guarantor gave the opinion to ANAC on the "Guidelines on the protection of the authors of reports of crimes or irregularities of which they have become aware due to an employment relationship, pursuant to art. 54-bis of Legislative Decree 165/2001 (so-called whistleblowing) ", where express reference is made" to the main obligations provided for by the legislation on the protection of personal data (articles 13, 14, 30, 35 and 36 of the Regulation), also taking into account the specific risks for the rights and freedoms of the data subjects in the workplace ").

As clarified recently by the Guarantor precisely with reference to the treatments carried out through applications for the acquisition and management of illegal reports (see provision June 10, 2021, n. 235, web doc. N. 9685922, spec. Par. 3.3), the processing of personal data carried out in this context - due to the particular delicacy of the information processed, as well as the high risks, in terms of possible retaliatory and discriminatory effects, even indirect, for the whistleblower, whose identity is protected by a specific regime of guarantee and confidentiality provided for by sector legislation (both at national and European level, see, most recently, Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report violations of Union law) - presents specific risks to the rights and freedoms of data subjects. This, also considered, the "vulnerability" of the data subjects (reporting and reported subjects) in the workplace (see articles 35 and 88, paragraph 2, of the Regulation; "Guidelines concerning the impact assessment on data protection as well as criteria to establish whether a treatment "may present a high risk" pursuant to Regulation 2016/679 ", WP 248 of 4 April 2017; see, most recently, provision of 4 December 2019, web doc. no. 9215763, with the which the Guarantor has given the opinion to ANAC on the outline of "Guidelines for the protection of the authors of reports of crimes or irregularities of which they have become aware due to an employment relationship, pursuant to art. 54-bis of Legislative Decree 165/2001 (so-called whistleblowing) ", where express reference is made to" the main obligations provided for by the legislation on the protection of personal data (articles 13, 14, 30, 35 and 36 of the Regulation), also taking into account the specific risks to the rights and freedoms of those concerned ti in the workplace ").

In acknowledging that, following specific investigations carried out during the investigation, the Company, albeit belatedly, carried out an impact assessment on data protection pursuant to art. 35 of the Regulation (see Annex D to the note of XX), it must be concluded that, until the preparation of the same, the treatment was carried out in the absence of an impact

assessment necessary to identify specific measures to mitigate the risks deriving from the treatment, in violation of art. 35 of the Regulation.

4. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the data controller in the defense writings □ whose truthfulness may be called upon to answer pursuant to art. 168 of the Code □ although worthy of consideration and indicative of the full cooperation of the data controller in order to mitigate the risks of the processing, compared to the situation present at the time of the investigation, they do not, however, allow to overcome the findings notified by the Office with the act of initiation of the procedure and are therefore insufficient to allow the filing of this proceeding, since none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

Although as stated, lastly, during the hearing with the Guarantor "no report of illegal conduct was acquired and processed through the whistleblowing application subject to the inspections", the Company has in any case carried out processing of personal data , as ascertained during the investigation and confirmed by the Company itself (see paragraph 3.3 of this provision), by recording and storing, within the logs of the firewall devices, information relating to the connections to the application in question by users, even if only related to the mere access and consultation of the application's web pages.

In order to determine the applicable law, in terms of time, the principle of legality referred to in art. 1, paragraph 2, of the l. n. 689/1981, according to which the laws that provide for administrative sanctions are applied only in the cases and times considered in them. This determines the obligation to take into account the provisions in force at the time of the committed violation, which in the case in question - given the permanent nature of the alleged offenses - must be identified in the act of cessation of the unlawful conduct. In acknowledging that the data controller has, during the investigation, taken steps to conform the treatment to the principles of the Regulation, to adopt appropriate technical and organizational measures to guarantee a level of security adequate to the risk presented by the treatment, as well as to carry out a specific impact assessment on data protection, it is believed that, given the cessation of unlawful processing which occurred after the date on which the Regulation became applicable (see note of the XX in which account is taken of the various initiatives taken by the owner to remedy for alleged violations), the Regulations and the Code constitute the legislation in the light of which to evaluate the treatments in question.

The preliminary assessments of the Office are therefore confirmed and the unlawfulness of the processing of personal data

carried out as it occurred in violation of Articles 5, par. 1, lett. a) and f), 13, 14, 25, 30, 32 and 35 of the Regulation.

The violation of the aforementioned provisions also makes the administrative sanction applicable pursuant to art. 58, par. 2, lett. i), and 83, para. 4 and 5, of the Regulation.

In this context, considering that the conduct has exhausted its effects, the conditions for the adoption of 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 ancillary sanctions (Articles 58, paragraph 2, letter i), and 83 of the Regulations; art. 166, paragraph 7, of the Code).

The Guarantor, pursuant to art. 58, par. 2, lett. i), and 83 of the Regulations as well as art. 166 of the Code, has the power to "inflict an administrative pecuniary sanction pursuant to Article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, depending on the circumstances of each single case "and, in this context," the College [of the Guarantor] adopts the injunction order, with which it also disposes with regard to the application of the ancillary administrative sanction of its publication, in whole or in excerpt, on the website of the Guarantor pursuant to Article 166, paragraph 7, of the Code "(Article 16, paragraph 1, of the Guarantor Regulation no. 1/2019).

In this regard, taking into account art. 83, par. 3, of the Regulations, in this case the violation of the aforementioned provisions is subject to the application of the same administrative fine provided for by art. 83, par. 5, of the Regulation.

The aforementioned administrative fine imposed, depending on the circumstances of each individual case, must be determined in the amount taking into account the elements provided for by art. 83, par. 2, of the Regulation.

For the purposes of applying the sanction, the nature, object and purpose of the processing were considered, the sector discipline of which provides, to protect the interested party, a high degree of confidentiality with specific regard to the identity of the same.

On the other hand, it was considered that, as declared by the Company, at the time of the inspections there were no reports of illegal conduct within the application in question, a circumstance that does not exclude the processing of data in any case carried out (see , in particular, par. 3.3 of this provision) and that the Company has provided a particular collaboration during the investigation by adopting, already following the inspection activity conducted by the Office, technical and organizational measures aimed at conforming the treatments in progress to the regulations on the protection of personal data, in compliance with the principle of accountability. It was also taken into account that specific clarifications regarding the need to carry out an

impact assessment on data protection in relation to the treatments in question were provided by the Guarantor as part of the aforementioned opinion given to ANAC on 4 December 2019, i.e. after carrying out the inspection activities at the Company.

The particular situation in which the Company was in during the period in which the preliminary investigation was carried out and the serious difficulties, also on an organizational level, that the Health Authorities had to face in the context of the epidemiological emergency were also taken into consideration. from SARS-CoV-2.

Furthermore, there are no previous violations committed by the data controller or previous provisions pursuant to art. 58 of the Regulation.

Due to the aforementioned elements, assessed as a whole, it is considered to determine the amount of the financial penalty, in the amount of 40,000.00 (forty thousand) euros for the violation of Articles 5, par. 1, lett. a) and f), 13, 14, 25, 30, 32 and 35 of the Regulation.

Taking into account the particular nature of the personal data being processed and the related risks for the reporting party and other interested parties in the workplace, it is also believed that the additional sanction of publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7, of the Code and by art. 16 of the Guarantor Regulation n. 1/2019.

Finally, it is believed that the conditions set out in art. 17 of Regulation no. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

WHEREAS, THE GUARANTOR

notes the unlawfulness of the treatment carried out by the Perugia hospital for the violation of Articles 5, par. 1, lett. a) and f), 13, 14, 25, 30, 32 and 35 of the Regulations, within the terms set out in the motivation;

ORDER

to the Perugia Hospital, in the person of the pro-tempore legal representative, with registered office in the Hospital of Santa Maria della Misericordia Sant'Andrea delle Fratte, 06156 Perugia, tax code / VAT number 02101050546, pursuant to Articles 58, par. 2, lett. i), and 83, par. 5, of the Regulations, to pay the sum of € 40,000.00 (forty thousand) as a pecuniary administrative sanction for the violations indicated 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 thirty days, an amount equal to half of the sanction imposed;

INJUNCES

to the Perugia hospital to pay the sum of € 40,000.00 (forty thousand) in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, according to the methods indicated in the annex, within thirty days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the l. n. 689/1981;

HAS

the publication of this provision on the website of the Guarantor pursuant to art. 166, paragraph 7, of the Code;

the annotation of this provision in the internal register of the Authority, provided for by art. 57, par. 1, lett. u), of the Regulations, violations and measures adopted in compliance with art. 58, par. 2, of the Regulation.

Pursuant to art. 78 of the Regulation, of art. 152 of the Code and 10 of Legislative Decree 1 September 2011, n. 150, against this provision, it is possible to appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the applicant resides abroad.

Rome, April 7, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei