SEE NEWSLETTER OF 11 MAY 2022

[doc. web n. 9768387]

Injunction order against ISWEB S.p.A. - April 7, 2022

Record of measures

n. 135 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 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 "".

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 via 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 ensure 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 records of the processing activities, carried out as data controller and data processor, are kept by the Company in electronic format (see Annex 1 to the minutes of the XXth);

- "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. 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 showing the roles of the two companies in the processing of personal data "(See annex 7 to the minutes of the XX; see the act of appointment of Seeweb S.r.l., attached to the following note of the XX).

With a XXth note, 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 Regulations, 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 24 November 1981).

With the aforementioned note, the Office found that the processing in question was carried out in the absence of a suitable discipline of the relationship with Seeweb S.r.l. to which the Company has used both for the treatments put in place as owner, in violation of art. 28, para. 1 and 3 of the Regulations, both for those carried out as a manager on behalf of its customers, including the Perugia hospital, in violation of art. 28, para. 2 and 4, of the Regulation.

With a note dated the XXth, the Company sent its defense briefs, declaring, among other things, that:

- "the alleged violations concern purely formal elements, since there have been no incidents that compromised the integrity, availability and confidentiality of the data processed by the Perugia Hospitals [...] ISWEB did not commit the alleged violations [...] the violations would be of purely formal nature and, in any case, without offensiveness since the substantial management of the technological infrastructure meets strict security criteria such as those provided by the Agency for Digital Italy and the Code of Conduct for Cloud Infrastructure Service Providers ";
- “the whistleblowing platform certified by Seeweb is accessible only through the public IPs of the Perugia Hospitals which convey the internal IPs via NAT. […] The configuration of the service foresees that the Perugia Hospitals reach the Whistleblowing platform through their three public IPs on which the tested IPs of the structures converge in NAT. As a result, Seeweb sees only and exclusively public IPs that cannot be associated with internal networks pass through. These IPs refer to a legal person and therefore their processing is not regulated by the legislation on the protection of personal data. Furthermore, neither Seeweb nor ISWEB process additional data which, associated with the IP numbers, make it possible to identify or make identifiable users who access the whistleblowing platform ";
- “neither Seeweb nor ISWEB process additional data which, associated with IP numbers, allow users who access the whistleblowing platform to be identified or made identifiable. It follows that neither of the two companies is carrying out processing of personal data. The EU Court of Justice, in fact, stated that IP numbers are not necessarily personal data, but that they become personal data if the owner can concretely associate them with other data that make users identified or identifiable ";
- "the IP numbers in question are excluded from the definition of personal data since it is not possible, even by crossing with other data, to identify or make a natural person identifiable";
- "also in consideration of the fact that the entire service does not imply a delegation to the processing of personal data, ISWEB did not have to stipulate the data processing agreement with Seeweb, did not have to obtain the authorization of the

Perugia Hospitals and should not have informed them of the presence of Seeweb ";

- the Company "has clearly described the technical structure of the service at the Perugia Hospitals indicating the presence of Seeweb as a provider of the cloud infrastructure before the conclusion of the contract. Consequently, with the acceptance of the offer and the execution of the contract, the Perugia Hospitals authorized the method of providing the service in Saas mode also through Seeweb ";

- "given that the object of the contract with the Perugia Hospitals is not the processing of the data of the reports but only the provision of a technological infrastructure, neither ISWEB nor Seeweb can take cognizance of the data of the reports that are encrypted with a key exclusively available to the hospitals of Perugia ";

- "the subject of the contract between ISWEB and the Perugia Hospitals does not concern the processing of data generated by the Saas platform but the provision of the Whistleblowing service according to the characteristics indicated in the commercial offer and in the technical annexes. It follows that the processing of IP numbers (which, it is repeated, in this case are not personal data and in any case are assigned to a public body) are not processed by the Perugia Hospitals. As a further consequence, also for this reason the stipulation of a sub-processor contract with Seeweb was not due. Furthermore, it should be considered that neither the GDPR nor the Personal Data Code provide for a specific formality to inform the data controller about the ways in which the services are provided, rather noting the actual knowledge of what happens. In this specific case, the Perugia Hospitals were aware of the existence of Seeweb and the use of its infrastructures since the circumstance was well highlighted in the commercial offer. Therefore, the Perugia Hospitals were informed of the existence of Seeweb at the time of stipulation and, with the stipulation, authorized (if ever necessary) the use of the sub-processor. Proof that the information in question was known to the Perugia Hospitals is in the "Technical Assistance" document (Annex 1) an integral part of the commercial offer. Specifically, on page 7 it is clarified that the ISWEB network server infrastructure is provided by Seeweb S.r.l .. ";

- "even in the case of the relationship between ISWEB and Seeweb, the agreement pursuant to art. 28 GDPR was not necessary. ISWEB, in fact, purchases from Seeweb the infrastructure necessary to operate the whistleblowing platform, without delegating either the definition of the purposes or the methods of processing to Seeweb ";

- "Isweb does not process the data of the reports which are encrypted and in the exclusive availability of the Perugia Hospitals [...] in no way can Seeweb acquire information on the acquisition and management of illegal conduct since the connection with

the whistleblowing platform always occurs with the same public IP of the structure concerned and, in any case, it is not possible to associate the IP that connects to the platform with the report. These circumstances, as well as the general functioning of the whistleblowing platform, were and are perfectly knowable by the Perugia Hospitals also in consideration of the fact that the platform in question is regulated by a license that allows free access to the source codes. Consequently, the Perugia Hospitals were and are in a position to know exactly all the necessary characteristics to its own regulatory compliance ";

- "as part of the review of its commercial processes, ISWEB has started an activity of further clarification of the method of supplying services in as a service mode consisting of the repetition of the information on the use of Seeweb contained in the technical documentation also in the offer commercial and providing for an express acceptance of the method of providing the service in place of acceptance through contractual stipulation ".

The hearing requested by the Company was also held on the 20th, pursuant to art. 166, paragraph 6, of the Code, following which the Company provided the Authority with "a copy of the e-mail message sent on December 17, 2015 to the Perugia Hospital, to which, among others, the document technician called "Server Network ISWEB", which clearly shows the infrastructure used for the provision of the service "(see note of XX and related annexes).

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 (provisions 10 June 2021, n. 235, web doc. 9685922, and n. 236, web doc. 9685947; see newsletter n. 480 of 2 August 2021, web doc. 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 of European delegation 2021 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).

In this framework, the subjects obliged to comply with the aforementioned provisions must process the data necessary for the acquisition and management of the reports in compliance also with the regulations on the protection of personal data (spec. Art. 6, par. 1, lett.), 9, par. 2, lett. b), 10 and 88, par. 1, of the Regulation).

In general, although the data controller, who determines the purposes and methods of data processing, has a "general responsibility" for the treatments put in place (see Article 5, paragraph 2, so-called "accountability", and 24 of the Regulation), even when these are carried out by other subjects "on its behalf" (cons. 81, art. 4, point 8), and 28 of the Regulation), the

Regulation has governed the obligations and other forms of cooperation to which the person in charge of the processing and the scope of the related responsibilities is held (see articles 30, 32, 33, par. 2, 82 and 83 of the Regulation).

The data processor is entitled to process the data of the interested parties "only on the documented instruction of the owner" (Article 28, par. 3, letter a), of the Regulation) and the relationship between the owner and manager is governed by a contract or by another legal act, stipulated in writing which, in addition to mutually binding the two figures, allows the owner to give instructions to the manager also from the point of view of data security and provides, in detail, what the subject matter is governed, the duration, the nature and purposes of the processing, the type of personal data and the categories of data subjects, the obligations and rights of the owner and manager. Furthermore, the data controller must assist the owner in ensuring compliance with the obligations deriving from the data protection regulations, "taking into account the nature of the processing" and the specific regime applicable to the same (Article 28, paragraph 3, letter f), of the Regulation).

In this context, the person in charge may not have recourse to another person in charge "without the prior written, specific or general authorization of the data controller" and, in this case, "the same obligations are imposed on this other data controller [...] in subject of data protection, contained in the contract or other legal act between the controller and the data controller "(Article 28, paragraphs 2 and 4, of the Regulation).

3.1. The treatments carried out by the Company on behalf of the Perugia Health Authority: failure to regulate the relationship with the hosting service provider.

For the purposes of compliance with the legislation on the protection of personal data, it is necessary to precisely identify the subjects who, for various reasons, can process personal data and clearly define their respective powers, in particular that of the owner, manager and other managers of the treatment, as well as the subjects who operate under the direct responsibility of these (articles 4, points 7) and 8), 24, 28, 29 and 32, par. 4, of the Regulation and art. 2-quaterdecies of the Code).

During the inspection it emerged that the Company "entrusted the company Seeweb S.r.l. the hosting service of the IT systems that host, among others, the whistleblowing application "(see Annex 7 to the minutes of the XXth).

Although the Company has declared that "the object of the contract with the Perugia Hospitals is not the processing of the data of the reports but only the provision of a technological infrastructure" and that "neither ISWEB nor Seeweb can take cognizance of the data of the reports that are encrypted with a key exclusively available to the Hospitals of Perugia ", concluding that" the entire service does not imply a delegation to the processing of personal data "also due to the fact that"

neither Seeweb nor ISWEB process additional data that, associated with IP, allow users who access the whistleblowing platform to be identified or made identifiable ", it must be considered that the operations described above still give rise to the processing of personal data pursuant to art. 4, point 2), of the Regulations for the reasons set out below.

The information contained in the reports of illegal conduct acquired through the "whistleblowing" application in question, albeit subject to encryption - which constitutes an effective measure that the owner and manager, also based on the principles of data protection by design and by default, they can adopt to make personal data incomprehensible to anyone not authorized to access it, guaranteeing the security of the processing and protecting the rights and freedoms of the data subjects - they must be considered as personal data as they represent information about persons identifiable physical persons (see cons. 83, and articles 4, point 1), 25 and 32, par. 1, lett. a), of the Regulation).

As clarified by the Guarantor on numerous occasions, also taking into account the guidelines of the European Data Protection Board (see Guidelines 7/2020 on the concepts of controller and processor in the GDPR, adopted by the European Data Protection Board on 7 July 2021, in particular, par. 2.1.4, point 40, in the part where the example relating to "Hosting services" is reported), the hosting service provider (in this case, a hosting service of virtual or physical servers), while not processing the IP addresses relating to the interested parties who use the application in question and while not directly accessing the personal data processed through this application, retains the latter on its technological infrastructure and guarantees its integrity and availability, adopting adequate technical and organizational measures, ensuring certain levels of service in terms of system availability and making available to its customers provides a series of tools to manage and monitor the service (see, with regard to the failure to regulate the relationship with the hosting service provider, prov. 10 February 2022, n. 44, forthcoming, and provision. 11 February 2021, n. 49, doc. web n. 9562852, spec. par. 3.2).

On the assumption that the data processed by the hosting service provider did not constitute personal data, the Company deemed it not required to "enter into the data processing agreement with Seeweb" and not to "obtain the authorization of the Perugia Hospitals" nor to having to inform the customer "of the presence of Seeweb".

In fact, from the examination of the documents in place, the relationship with Seeweb S.r.l. to which the Company has used both for the treatments put in place as owner (profile in relation to which see the following paragraph; see Article 28, paragraphs 1 and 3, of the Regulation), and for those carried out as a manager on behalf of its customers, including the Perugia hospital (see Article 28, paragraphs 2 and 4, of the Regulations).

In acknowledging the fact that the appeal to Seeweb S.r.l. as provider of the hosting service had been indicated in the technical documentation made available, before the conclusion of the contract, by the hospital of Perugia, which therefore could not be considered completely unaware of the involvement of another subject in the overall treatment, it is however necessary draw attention to the provisions of art. 28, par. 2, of the Regulations, which expressly requires that the person in charge not have recourse to another person in charge “without the prior written authorization, specific or general, of the owner”, an authorization which, in this case, has not been acquired.

This provision is, in fact, functional to ensure that the data controller always has full control of the treatments that are carried out on his behalf, being able, if necessary, to oppose both the very possibility of resorting to "other data processors", and the identification of these subjects as carried out by the "initial manager" (see Article 28, paragraphs 2 and 4, of the Regulation).

Although during the investigation the Company regulated the relationship with Seeweb S.r.l. on 18 September 2019, designating it as the data processor (see note of XX), it is noted, however, that the document transmitted does not take into account the role of sub - manager hired by Seeweb S.r.l. with regard to the treatments carried out on behalf of the Company's customers, including that relating to the acquisition and management of illegal conduct using the application used by the Perugia hospital.

For these reasons, it is believed that the Company's use of the services offered by Seeweb S.r.l. - in the absence of a contract or other legal act governing the processing of personal data, by the latter, as a sub-processor, and without specific authorization from the Company regarding the involvement of this subject - it is occurred in violation of art. 28, para. 2 and 4, of the Regulation.

3.2. The treatments put in place by the company as data controller: failure to regulate the relationship with the hosting service provider.

As highlighted in the previous paragraph, from the examination of the documentation provided, it appears that the roles assumed with regard to the processing of personal data carried out by the hosting service provider had not been defined in the "General contract for the supply of Seeweb services" or in other legal acts, not being regulated, pursuant to art. 28, para. 1 and 3 of the Regulation, the relationship with Seeweb S.r.l. to which the Company has also made use of the numerous treatments put in place as owner and, therefore, attributable to heterogeneous purposes (from the management of the employment relationship with its employees, to the accounting and administrative management, to the instrumental treatments to provision

of its services) which, by their very nature, may involve the processing of even particular categories of personal data and also involve "vulnerable" interested parties.

With a note of the twentieth, the Company, however, sent a copy of the deed of the twentieth with which it intended to regulate the relationship with Seeweb S.r.l., designating it in charge of the treatment, limited to the treatments carried out on its own behalf.

In this regard, it is essential to remember that the owner, in the context of the preparation of the technical and organizational measures that meet the requirements established by the Regulation, also from the point of view of safety (articles 24 and 32 of the Regulation), can use a manager to the performance of some processing activities, to which it gives specific instructions (see recital 81 of the Regulation). In this case, the owner "only resorts to data processors who present sufficient guarantees to put in place [the aforementioned measures] adequate so that the treatment meets the requirements of the Regulation and guarantees the protection of the rights of the data subjects" (art. 28 , par. 1, of the Regulation. Pursuant to art. 28 of the Regulation, the data controller can therefore also entrust processing to external subjects, regulating the relationship with a contract or another legal act and giving instructions on the main aspects of the treatment (art. 28, par. 3, of the Regulation) and the person in charge of the treatment is therefore, in turn, entitled to process the data of the interested parties "only on the documented instruction of the owner" (art. 28, par. 3, letter a) of the Regulation.

In such cases, the data protection regulations require that the relationship between the owner and the hosting service provider be governed by a contract or other legal act pursuant to art. 28 of the Regulation (see also recital 81 and art. 4, point 8, of the Regulation), also in order to avoid processing (communication to third parties) in the absence of a suitable prerequisite of lawfulness (given the notion of "third party" referred to in 'Article 4, point 10, of the Regulation; see Article 2-ter, paragraphs 1 and 4, letter a), of the Code, with regard to the definition of "communication").

Nevertheless, with regard to the present case, the relationship between the Company, as data controller, and the hosting service provider has been regulated in terms of data protection only following the inspection activity conducted by the Guarantor (with regard to the specific risks deriving from the failure to regulate the relationship, pursuant to art.28 of the Regulation, with the subjects who process the data on behalf and in the interest of the data controller, provision 17 September 2020, n.160 and 161, web doc. No. 9461168 and 9461321; see also provision 11 February 2021, no. 49, web document no. 9562852, provision 17 December 2020, no. 280, 281 and 282, web document no. 9524175, 9525315 and 9525337, as well as

provisions of 10 February 2022, no. 43, web doc. No. 9751498, provision of 10 February 2022, no. 44, forthcoming, cit.).

Given the above, taking into account the considerations made in the previous paragraph regarding the processing carried out by the hosting service providers and the fact that, at least until 19 September 2019, the Company has failed to regulate the processing of personal data carried out, on its own behalf. and in its own exclusive interest, by an external party (in this case the hosting service provider), it is believed that the Company is responsible for the violation of art. 28, para. 1 and 3 of the Regulation.

4. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the data controller in the defensive writings for the veracity of which one may be called to answer pursuant to art. 168 of the Code although deserving 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.

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 violation committed, which - given the permanent nature of the alleged offenses - is still ongoing. Therefore, it is believed that the Regulation 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 is noted, since the Company has not regulated the relationship with the hosting service provider to which the Company has resorted both for the treatments carried out in as owner, in violation of art. 28, para. 1 and 3 of the Regulations, both for those carried out as a manager on behalf of its customers, including the Perugia hospital, in violation of art. 28, para. 2 and 4, 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, par. 4, of the Regulation.

5. Corrective measures (art. 58, par. 2, letter d), of the Regulation).

Considering that, to date, the Company has not proved that it has regulated the relationship with the hosting service provider in relation to the treatments carried out on behalf of the Perugia hospital through the application used for the acquisition and management of reports of alleged offenses, by not previously acquiring the authorization of the owner, it is necessary to order the Company, pursuant to art. 58, par. 2, lett. d), of the Regulation, to conform the processing to the provisions on the protection of personal data (Article 28, paragraphs 2 and 4, of the Regulation), within thirty days of notification of this provision.

Pursuant to art. 58, par. 1, lett. a), of the Regulation and 157 of the Code, the Company must also communicate to this Authority, providing an adequately documented feedback, within thirty days from the notification of this provision, the initiatives undertaken to ensure compliance of the treatment with the Regulation.

6. 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).

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, with regard to the processing of data carried out on behalf of the Perugia hospital, the nature, object and purpose of the processing whose sector regulations provide for the protection of the interested party were considered. , a high degree of confidentiality with specific regard to the identity of the same. On the other hand, it was considered that at the time of the inspections there were no reports of illegal conduct within the application for the acquisition and management of reports of offense and that in the documentation provided in the pre-contractual phase to the company the appeal had been indicated to the services offered by the company Seeweb s.r.l., thereby allowing to presume that the Company was at least aware of the involvement of another subject in the overall treatment.

With regard to the treatments carried out as owner, it was considered that the Hosting service, entrusted without the supplier's

role having been previously regulated in accordance with the data protection regulations, concerned the multiple treatments that the Company carries out as owner. for different purposes (from the management of the employment relationship with its employees, to the accounting and administrative management, to the instrumental treatments for the provision of its services) which, by their nature, may involve the processing of even particular categories of personal data and involve also affected "vulnerable". On the other hand, it was considered that after the inspection the Company proceeded to regulate the aforementioned relationship pursuant to art. 28 of the Regulation and which do not appear, previous violations committed by the same or previous provisions pursuant to art. 58 of the Regulation.

Due to the aforementioned elements, assessed as a whole, it is believed to determine the amount of the financial penalty, in the amount of € 40,000.00 (forty thousand) for the violation of art. 28 of the Regulation, given that, in relation to the specific case, the sanction is effective, proportionate and dissuasive (Article 83, paragraph 1, 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

detects the unlawfulness of the processing carried out by ISWEB S.p.A. for the violation of art. 28 of the Regulations, within the terms set out in the motivation;

ORDER

to ISWEB S.p.A., in the person of the pro-tempore legal representative, with registered office in Via Tiburtina Valeria Km. 112,500, 67068 Scurcola Marsicana (AQ), tax code / VAT number 01722270665, pursuant to articles 58, par. 2, lett. i), and 83, par. 4, 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 ISWEB S.p.A:

a) 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;

b) pursuant to art. 58, par. 2, lett. d), of the Regulation, to conform, within the terms described in point 5 of this provision, the treatments to the provisions on the protection of personal data (Article 28, paragraphs 2 and 4, of the Regulation), within thirty days of notification of this provision;

c) pursuant to art. 58, par. 1, lett. a), of the Regulation and 157 of the Code, to communicate to this Authority, providing an adequately documented feedback, within thirty days from the notification of this provision, the initiatives undertaken to ensure compliance of the treatment with the Regulation;

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 the 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