[doc. web n. 9813326]

Order injunction against Acqua Novara.VCO S.p.a. - July 21, 2022

Record of measures

n. 269 of 21 July 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 whistleblower, were carried out - 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 - specific investigations against Clio S.r.l. (hereinafter "Clio" or "Supplier") which supplies and manages on behalf of various subjects, public and private, the application used for the acquisition and management of reports of illegal conduct (see reports of operations carried out in the XXth ).

During the inspection it was ascertained that the aforementioned application is also used by Acqua Novara.VCO S.p.a. (hereinafter "ANVCO" or "Company").

2. The preliminary activity.

During the inspection at the Supplier, the following emerged:

Clio provided a list of clients, including the Company, to whom "it offers the service for the acquisition and management of reports of illegal conduct and represented that [...] does not make use of sub-managers for the execution of activities of treatment "(see minutes of the XXth, p. 3 and annex 3);

Clio has been designated as data processor only by some customers, while others, including the Company, "have not identified the Company as the data processor pursuant to art. 28 of the Regulations "(see minutes of the XX, p. 3 and annex 4, 5 and 6);

"The whistleblowing application, reachable from the public network at a web address such as" https://nomeente.whistleblowing.name ", is made available to customers in Software as a Service (SaaS) mode. This method of providing the service, in the opinion of the Company, represents a specific guarantee to protect the identity of the reporting parties as it allows the management of data by a person other than the employer administration. The application in question, developed by Clio, is installed on a server at the Company's data center and is configured in multitenant mode. The application only allows the acquisition of reports by employees and does not allow the acquisition of anonymous reports or by subjects external to the administrations. Since some customers have represented the need to also acquire anonymous reports or reports from external parties, the Company is developing a new version of the application that will also allow the acquisition of these types of reports and which will be put into production during the year 2020. The Company provides assistance and

maintenance services "(see minutes of XX, p. 4);

"When activating the service for a new entity, [Clio] creates [...] the key used to encrypt the data relating to the reports stored in the application database in the production environment" (see minutes of the XX, p. 5).

Subsequently, with a note of the XXth, the Supplier, in addition to the documentation and information provided during the inspection activity, communicated that he "sent to [...] Customers who have not yet done so, a reminder via pec for the conferment of the appointment of Clio as Outsourced Data Processing Manager, communicating that, in the absence of a reply within seven working days, we would have suspended the service until regularization "(p. 1).

Lastly, in response to a specific request for information by the Office, the Supplier, on XX, further specified that the relationship with ANVCO - for which, at the time of the inspection activities, had been acquired through the application in question at least one real report of unlawful conduct not attributable, therefore, to mere testing or verification of the operation of the application) - has been governed pursuant to art. 28 of the Regulation "following the reminder pec" sent by the Supplier.

With a XXth note, the Office, on the basis of the elements acquired, notified ANVCO, 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 ANVCO has put in place the processing of personal data of employees and other interested parties, through the use of the application for the acquisition and management of illegal reports, not having regulated the relationship with the Supplier, in violation of art. 28 of the Regulation; making available to the same Supplier data relating to reports of offenses in the absence of an appropriate legal basis, in violation of Articles 5, par. 1, lett. a), and 6 of the Regulations and art. 2-ter of the Code; and not having communicated the contact details of the data protection officer to the Guarantor, in violation of art. 37, par. 7, of the Regulation.

With a note of the twentieth, ANVCO sent its briefs specifying, among other things, that:

“ANVCO manages the integrated water service in 140 Municipalities of the Provinces of Novara and Verbano-Cusio-Ossola and is present in the area with 14 operational offices. ANVCO is a company controlled by the P.A. and as such it has adopted both the corruption prevention systems and the organization, management and control model pursuant to Legislative Decree

231/2001, as per ANAC provisions on the subject from time to time. This is premised because, as will be said, the reference prevention regulations were used by the undersigned Company to evaluate and justify the selection of the system and the supplier, as well as the privacy roles of the subjects involved in the possible processing of personal data ";

"In November 2018, a team composed of the then head of the IT Office and the Head of Corruption Prevention and Transparency (RPCT) identified the application in question as suitable to meet the needs of the Entity to effectively manage whistleblowing reports ";

"The purchase order was signed on January 16, 2019 [...] and at the beginning of June 2019 the Board of Directors of ANVCO approved the update of the internal policy for whistleblowing [...] . The making available of the application and the release of the updated policy were also accompanied by a training activity addressed to all staff which highlighted, among others, the guarantees that the current regulatory framework offers to the whistleblower ";

"On 3 July 2019 the application actually" went into operation "and, subsequently, on the 20th, the undersigned Company received a message of p.e.c. with which the Clio supplier requested the formulation of the deed of appointment as data processor. Following the agreements with the supplier, the document was formalized on 3 December 2019 ";

"The contractualization with the supplier took place initially - for the period between 3 July 2019 and 3 December 2019 - without formalizing the appointment of the data processor. This choice was made following an analysis of the regulatory framework and of the factual circumstances that led to the inclination for an "autonomous" ownership of the supplier itself ";

"Research carried out at the time did not reveal any provisions of this Most Illustrious Authority on the subject, except for a report to Parliament in 2009 in which regulatory measures were hoped to provide legitimacy support for the treatments that could be hypothesized for the reporting systems in question , and a position of the Article 29 Group cited therein which - examining the possibility of using external suppliers - stated "The companies or groups of companies that entrust part of the management of the reporting system to external suppliers remain responsible for the processing operations that result as the external suppliers operate solely as data processors pursuant to Directive 95/46 / EC. External suppliers can be companies that manage call centers or companies or law firms specialized in collecting complaints and sometimes appointed to carry out part of the necessary verification activities ";

"In the context of the assessments formulated within the Entity until July 2019 (and beyond), the circumstance of an apprehension, albeit occasional, of a personal data relating to the whistleblower / report would never have occurred, not even

during the maintenance phase of the system (since the data is encrypted), since any apprehension would have entailed criminal liability for its employee (the maintenance technician) and, for the supplier company, contractual liability (there would have been a lack of expected measures) ";

"Having considered that Clio could rightfully operate as an" autonomous "owner therefore seemed, in the light of the above research, an adequate solution to respect the principle of effectiveness (impact in determining the methods of treatment) and at the same time a way to prevent Clio from the interference that the owner is required to put in place towards the manager (through instructions and checks for example). Such interference could hypothetically have represented threats to the secrecy and confidentiality of the reporting party's personal data and in the concrete undermine the trust of users in the use of the system as better explained in note 1 and in the aforementioned doctrine ";

"ANVCO's determination, however, was not reflected, at the end of November 2019, with the considerations that the Illustrious Authority had formulated during the inspection phase at Clio, the Entity had therefore promptly adhered to the proposed interpretation, after having received information from Clio , considering that - for the first time - it was a clear position on the subject by the Authority. This interpretation was reaffirmed in the same days by the Guarantor Authority, with provision of 4 December 2019 (web doc. No. 9215763), on the occasion of the favorable judgment on the adoption of "new" Guidelines by ANAC in the Guidelines ANAC, issued on 9 June 2021 on the basis of the provisions of art. 54-bis, co. 5, Legislative Decree n. 165/2001, the profiles concerning the reports made in the public sphere are examined in depth, aimed at allowing the administrations and other recipients of the same to correctly fulfill the obligations deriving from the personal data protection regulations. In chapter 2.2. dedicated to the "Methods of managing reports: computerized and traditional procedures", ANAC reiterates, as a priority method to protect the confidentiality of the whistleblower, the computerized management of reports, recognizing the supplier as an "authorized" role, which is then corrected in "Data processor" ";

"The regulatory framework in which ANVCO found itself operating at the time of the implementation of the Clio application was far from defined and the same, after carrying out the research and the above considerations, had considered that the legislative change made from Law no. 179/2017 had a prevalent character over that of regulatory rank, as also underlined in opinion no. 615/2020 issued by the Council of State on the outline of the Guidelines (Council of State, Section One, Section Meeting of March 4, 2020) ";

"The evaluations carried out by ANVCO, it must be reiterated, were also strong in the fact that the choice and characteristics of

the application, analytically described in the provision of the Guarantor Authority, are such as to ensure the adoption of a high level of security for the rights and the freedoms of the interested parties in compliance with the principles of integrity and confidentiality just described even where - initially - the Entity had considered the application provider as an independent data controller due to the peculiar characteristics of independence and autonomy that this role on the other hand, with respect to that of data controller, it ensures, in itself, contractually bound to the data controller with all the consequent obligations deriving from it, including the subjection to the powers of instruction, control and transparency in access rights, reserved by the Regulation (EU) 2016/679 to the data manager ";

"The data protection model by design and by default (privacy by design and by default) adopted by ANVCO through the choice of the technological solution provided by Clio, implements appropriate technical and organizational measures to guarantee an adequate level of security for risks presented by the processing carried out as part of the IT procedures for the acquisition and management of reports, allowing the data - primarily those of the reporting party - to be managed by a third party other than the administration, in compliance with the principles of secrecy and autonomy of the systems that allow workers to report - in safe conditions - any illegal or suspicious behavior of which they become aware ";

"A single report was acquired through the application in August 2019. Upon acceptance by the RPCT, this report was then archived as per the report that the SB sent to the Board on January 30, 2020 ";

"It is considered appropriate to point out that, regardless of the considerations on the relationship between ANVCO and Clio, any personal data present in the application: they are therefore not related to a whistleblower (as understood by Law no. 179/2017), they are also not related to a reported and / or unlawful or suspected offense (again as understood by Law no. 179/2017). Finally, there is no evidence, to the knowledge of the writer, that such personal data are available to employees / collaborators of Clio (or third parties) as their possible apprehension is technically averted by encryption, as well as protected by a penalty provision. penalty of the offender. The identity (personal data) of the whistleblower is not even known to the RPCT since, since the need did not exist (the report had no criminal relevance to the assessment of the RPCT and the ODV), access to said data was never performed ";

"There is a very short period of time between the actual activation of the anonymous reporting service (the XXth) and the appointment of the supplier as data controller, formalized on December 3, 2019";

"The only report of August 2019 was not relevant pursuant to Law no. 179/2017 and therefore the objective gravity is

considerably reduced in relation to the modalities and rank of the protected legal asset deriving from the apprehension of the information on the reported / whistleblower, of which in any case there is no evidence ";

"With reference to the violation of articles 5, par. 1, lett. a), 6 of the GDPR and art. 2-ter of the Privacy Code referring to the unlawful processing of personal data resulting from the communication deriving from having made available to the Supplier data relating to reports of offenses in the absence of an appropriate legal basis, the Exponent believes that this case has not in fact verified, as any personal data contained therein is encrypted and inaccessible to the supplier ";

the Company "has communicated the name and contacts of the DPO since his appointment in 2018, sending the appropriate communication acquired by this Most Illustrious Authority [...] Subsequently, ANVCO notified the change in the data of the data protection officer , by sending a further communication "on XX.

The hearing requested by ANVCO was also held on the 20th, pursuant to art. 166, paragraph 6, of the Code, on the occasion of which it was represented, among other things, that:

"The selection of the supplier of the aforementioned service took place in December 2018, a supplier with whom the Company entered into a service contract in January 2019; in the following months, up to June 2019, the Company carried out a series of preparatory activities for the activation of the online procedure for the acquisition and management of reports, defining the methods of use and carrying out a communication and training campaign towards of employees ";

"The service was activated on 3 July 2019 and in August 2019 a report was received which was processed by the Supervisory Body and the RPCT and subsequently archived";

"The other two reports that were present in the whistleblowing application at the time of the Authority's inspection at Clio S.r.l., which took place in November 2019, are presumably attributable to technical tests carried out by the Company";

"The assessments made by the Company in relation to the service provider in the processing of personal data were based on the qualified nature of the services offered by the same, as well as the sector framework which provides for specific criminal responsibilities in the event of disclosure of the identity of the reporting persons";

"The Company, also following a specific request from the supplier following the inspection by the Authority, then formalized the relationship with Clio S.r.l. pursuant to art. 28 of Regulation (EU) 2016/679 ".

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. no. 1693019; see, also, Working Group Art. 29, "Opinion 1/2006 on the application of EU legislation on data protection 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, web doc. 1607645).

In recent years, there have been numerous interventions by the Guarantor, including of a general nature, on the matter (see, most recently, provisions of 7 April 2022, nos. 134 and 135, web doc. Nos. 9768363 and 9768387 , and precedents referred to therein; see also provision no. 215 of 4 December 2019, web doc. no. 9215763, opinion of the Guarantor on the outline of "Guidelines for the protection of the authors of reports of crimes or irregularities referred to have become aware of an employment relationship, pursuant to Article 54-bis of Legislative Decree 165/2001 (so-called whistleblowing) "of ANAC)

During a hearing in Parliament, the Guarantor 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 "carry out a congruous balancing 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 in the exercise of the delegation "(see, Hearing of the Guarantor for the protection of personal data on the d.d.l. 2021 European Delegation, Senate of the Republic-14th Parliamentary Commission of the European Union, 8 March 2022, web doc. no. 9751458).

At the national level, 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 of 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 with the personal data protection regulations (spec. Art. 6, par. 1, letter c), 9, par. 2, lett. b), 10 and 88, par. 1, of the Regulations; on this point, see, most recently, provisions of 7 April 2022, nos. 134 and 135, doc. web nos. 9768363 and 9768387, 10 June 2021, nos. 235 and 236, doc. web nos. 9685922 and 9685947).

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).

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 10 June 2021, nos. 235 and 236, web doc. N. 9685922 and 9685947; see

newsletter n. 480 of 2 August 2021, web doc. 9687860 ; but see already provision. 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 in reason for an employment relationship, pursuant to Article 54-bis of Legislative Decree 165/2001 (so-called whistleblowing) "of ANAC).

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; see, among others, provision of 10 February 2022, n. 43 , web doc. no. 9751498 and the previous provisions referred to therein).

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 "(art. 5, par. 1, lett. f), of the Regulation).

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 regulate the relationship with the Supplier.

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 security (articles 24 and 32 of the Regulation), may use a person in charge for the performance of some processing activities. , to which it issues 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 , paragraph 1, of the Regulation. On this point it is noted that the data

controller is required to "implement adequate and effective measures [and to ...] demonstrate the compliance of the processing activities with the [...] Regulation, including the effectiveness of the measures ”adopted (cons. 74 of the Regulation).

Pursuant to art. 28 of the Regulation, the owner 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 processing, in particular, for the profiles of interest in this procedure. : “The duration of the processing”, “the obligations and rights of the data controller”, as well as the operations to be carried out “after the provision of the services relating to the processing has ended” (Article 28, par. 3, of the Regulation).

The data controller is therefore entitled to process the data of the interested parties "only on the documented instruction of the owner" (Article 28, paragraph 3, letter a), of the Regulation; in this regard, see Cass., Section I Civ., Ordinance no. 21234 of 23 July 2021).

In the present case, ANVCO, the data controller required to comply with the obligations deriving from the sector regulations, instead of independently creating an application for the acquisition and management of reports of offenses, has taken the decision to use the services offered by a company external supplier of the application. Therefore, the Supplier of the whistleblowing application has processed the personal data of the whistleblowers and other interested parties indicated in the reports (reported subjects, witnesses, etc.) as part of an instrumental service aimed at acquiring and managing reports of offenses, for account and in the interest of ANVCO which operated in the fulfillment of legal obligations imposed on the latter.

The functions performed by the Supplier therefore entailed the processing of the personal data of the whistleblowers and other interested parties indicated in the reports (reported subjects, witnesses, etc.) of which ANVCO is in any case the owner, treating them on the basis of a specific legal obligation and determining the means and methods of processing as well as the main terms of the execution of the service on the basis of specific contracts.

In such cases, the data protection regulations require that the relationship between the owner and the supplier 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"). Nonetheless, with regard to the case in point, the relationship between the Company and the Supplier has not been appropriately regulated from the point of view of data protection, as shown by the

documents in the file.

In relation to the profiles regarding the protection of personal data, it is noted that the service supply contract with the supplier (see Annexes 1 and 2 to the note of XX) does not have the specific characteristics of the legal act that defines the role of the manager, as it does not contain the elements provided for by art. 28 of the Regulation (see spec. Par. 3).

In this regard, what is highlighted in the defense statement regarding the reference to the role assumed by external suppliers in this area, which would operate "solely as data processors", cannot be considered relevant. This indication is reported inaccurately in an Italian translation of the document "Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime ", which instead in its English language version correctly qualifies external suppliers as data processors (" providers merely act as processors "). This, however, does not appear to have concretely affected ANVCO's assessments and organizational choices, given that the same declared that it initially considered that the Supplier operated as data controller.

It is therefore ascertained that - without prejudice to the assessments regarding the lawfulness of the processing carried out by the Supplier, subject to an independent procedure - ANVCO, from 3 July 2019 (date on which the application was made fully operational) to 3 December 2019 (date in which regulated the relationship with the Supplier), operated in violation of art. 28 of the Regulation, not having regulated the relationship with the Supplier in terms of data protection, in violation of art. 28 of the Regulation.

3.2 Unlawful processing of data relating to whistleblowing reports.

In light of the foregoing considerations and the documentation in place, in the period from 3 July to 3 December 2019, given the absence of a regulation of the relationship with the Supplier pursuant to art. 28 of the Regulation, ANVCO, making use of the services offered by it, in order to provide its structure with an effective and efficient system for the acquisition and management of reports of illegal conduct, as required by law, has made available to the Supplier the relative personal data to reports of illegal conduct, allowing them to collect and store them through the whistleblowing application, in the absence of a suitable regulatory requirement.

Although ANVCO declared that such data processing "did not actually occur [o], as the personal data possibly contained [... in the platform] encrypted and inaccessible to the supplier" and that "the circumstance of an apprehension would never occur , albeit occasional, of personal data relating to reporting / reporting, not even during system maintenance (being the data

encrypted) ", it must be considered that the use of encryption constitutes only 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 who is not authorized to access it, guaranteeing the security of processing and protecting the rights and freedoms of the data subjects. However, this does not exclude the possibility of processing personal data in this case. For these reasons, given the definition of "treatment" pursuant to art. 4, point 2), of the Regulation, and as recently clarified by the Guarantor, the information present in the reports of illegal conduct acquired through the application in question, even if subjected to encryption, must be considered as personal data as it represents information on identifiable natural persons (see cons. 83, and articles 4, point 1), 25 and 32, par. 1, lett. a), of the Regulations; on point v. prov. 7 April 2022, n. 135, doc. web n. 9768387, cit.).

In this regard, it is also not relevant that, after its acquisition, the report of illegal conduct, present in the whistleblowing application at the time of the Authority's inspection activities, was archived, without "the access "to the data relating to the identity of the reporting party. As is known, in fact, even the mere collection and storage of personal data configures a treatment subject to the rules on data protection (Article 4, point 2), of the Regulation).

Considering the failure to regulate the relationship with the Supplier in terms of data protection, it is believed that, as previously clarified by the Guarantor with regard to similar cases (see provision of 7 March 2019, n.81, web doc. n. 9121890; provision 17 September 2020, n. 160, web doc. n. 9461168; provision 17 December 2020, n. 280, web doc. n. 9524175; "Guidelines 07/2020 on the concepts of owner and manager of processing in the GDPR ", adopted on 7 July 2021 by the European Committee for the protection of personal data, spec. note 42), ANVCO has allowed processing operations and / or made available to the Supplier the personal data relating to reports of acquired offenses through the whistleblowing application, in the absence of an appropriate legal basis, resulting in unlawful processing, in violation of Articles 5, par. 1, lett. a), and 6 of the Regulations and art. 2-ter of the Code.

4. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the data controller in the defensive writings - the truthfulness of which one may be called 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.

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), 6 and 28 of the Regulations and art. 2-ter of the Code. During the procedure, the Company instead proved that it had communicated the contact details of its data protection officer to the Guarantor (which is why it is deemed necessary to file the related dispute profile).

The violation of the aforementioned provisions makes the administrative sanction applicable pursuant to art. 58, par. 2, lett. i), and 83, para. 4 and 5, of the Regulation and of Article 166, paragraph 2, of the Code.

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 Regulation, in the present case - also considering the reference contained in art. 166, paragraph 2, of the Code - 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 pecuniary sanction 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, for the protection of 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 ANVCO, at the time of the inspections there was only one report of illegal conduct within the application in question and that the violations carried out lasted for a few months (from 3 July to 3 December 2019). In addition, the Company collaborated 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 of the principle of accountability, governing the relationship with the Supplier pursuant to art. 28 of the Regulation. 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 believed to determine the amount of the financial penalty, in the amount of € 20,000.00 (twenty thousand) for the violation of Articles 5, par. 1, lett. a), 6 and 28 of the Regulations and art. 2-ter of the Code

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 treatment carried out by Acqua Novara.VCO S.p.a. for the violation of articles 5, par. 1, lett. a), 6 and 28 of the Regulations and art. 2-ter of the Code, in the terms set out in the motivation;

ORDER

to Acqua Novara.VCO S.p.a., in the person of the pro-tempore legal representative, with registered office in via Triggiani Leonardo 9, 28100 Novara, C.F./P. IVA 02078000037, pursuant to art. 58, par. 2, lett. i), and 83, par. 5, of the Regulations, to pay the sum of € 20,000.00 (twenty 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 Acqua Novara.VCO S.p.a., to pay the sum of € 20,000.00 (twenty 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 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, 21 July 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei