[doc. web n. 9811271]

Order injunction against Clio s.r.l. - July 21, 2022

Record of measures

n. 268 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, specific investigations have been carried out against Clio S.r.l. (hereinafter "Clio" or "Company"), which provides 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 the operations carried out by the XX).

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.

During the inspection at the Company, the following emerged:

the Company "provided a copy of the register of the processing activities carried out by the Company as data controller [...], representing that the same is kept [...] in electronic format", in which "the activity is recorded the provision of the whistleblowing service for which the company defines itself as the "Customer Manager" "(see minutes of the XX, p. 3 and annex 1);

"the Company, at present, has not yet established the register of the processing activities carried out as a manager on behalf of its customers" (see minutes of the XX, p. 3);

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

the Company has been appointed as data processor by some customers, while others "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);

"Access to the whistleblowing application is allowed through authentication credentials consisting of a username (usually an e-mail address) and a password. Five different authorization profiles have been envisaged: (1) "Application Administrator" profile, used by Company personnel, which allows the activation and deactivation of the various application instances as well as the creation of the user with the profile "Responsible"; (2) "Manager" profile, used by the RPCT of the entity, which allows the display and management of reports; (3) "Anti-corruption Staff" profile, used by the staff of the RPCT, which has a supporting role in the investigation management of the reports without the possibility of knowing the identity of the whistleblowers; (4) "User management" profile which only allows the management of utilities used by the staff of the institution and does not allow access to the data of the reports; (5) "Reporting" profile that allows the staff of the entity to make a report and check the processing status of their reports "(see minutes of XX, p. 4);

the Company highlighted that "each user can be assigned only one profile and that, where necessary, to assign multiple profiles to the same subject (for example, as reporting person and as a staff member of the RPCT) it is necessary to create distinct users, one for each profile "(see minutes of the XXth, p. 2);

the Company stated that "when activating the service for a new entity, it [...] 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 20th, p. 5);

the Company "has represented that, in the event of termination of the service supply contract, the Company makes available to the RPCT of the entity an encrypted export of the data of the reports acquired before the cancellation of the same" (see minutes of XX, p. 4).

Subsequently, with a note of the XXth, the Company, in addition to the documentation and information provided during the inspection activity, communicated that it had "sent to [...] Customers who have not yet done so, a reminder via certified e-mail 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 "and to have" modified the conditions of use and subjected the completion of the MEPA purchase to " acquisition of the appointment as Data Processors

pursuant to art. 28 GDPR "(p. 1 and annex 4).

Lastly, in response to a specific request for information by the Office, the Company, on XX, further specified that the relationships with customers - for which, at the time of the inspections, had been acquired through the 'application in question at least one real report of illegal conduct (therefore not attributable to mere testing or verification of the operation of the application) and for which the supply contract of the application in question was still in progress (Municipality di Ginosa and Acqua Novara.VCO S.p.a.) - have been governed pursuant to art. 28 of the Regulations "following the reminder pec" sent by the Company. The other contracts were instead concluded with the termination of the contract and the deactivation of the service.

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 - given the failure to regulate the relationship with certain customers, data controllers, pursuant to art. 28 of the Regulations - the processing of personal data put in place by the Company, up to the regulation of the relationship with customers, took place 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, as well as in the absence of keeping the register of processing activities carried out on behalf of the data controllers, in violation of art. 30, par. 2, of the Regulation.

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

"Most of the contracts for the service provided through the CLIO" Whistleblowing "application were activated in 2016/2017, immediately after the entry into force of the legislation on Whistleblowing in Italy and the ANAC guidelines of 2015 and before of the entry into force of EU Regulation no. 679/2016, in accordance with art. 29 of Legislative Decree 196/2003 which configured the appointment of the Data Controller as a "faculty" and not an obligation ";

"It is probably to be attributed to this reason the fact that in subsequent renewals - which took place through contacts between the respective administrative / accounting offices - the adaptation to art. 28 of the Regulations with a "formal" investiture of CLIO as Data Processor on the sidelines of the Supply Contract. However, the latter implied de facto such a role on the part of

the supplier which, as you could see in the Company's Register of Treatments, qualified as such. In the 2021 guidelines, ANAC also considers the service provider logically Responsible for the processing ";

"The Bodies that had appointed CLIO as manager had contracted the service for the first time in the course of 2019 in the force of the GDPR and, therefore, with procedures now standardized in the conclusion of contracts that provided for the acquisition of the nomination ex art. 28 of the GDPR also due to the establishment of the DPO, whose full operation required some time with respect to the date of entry into force of the Regulation (25 May 2018) ";

"In other cases, the absence of the appointment as Manager did not lead to damages and / or illegitimate treatment by CLIO or otherwise contrary to the principles of lawfulness, transparency and fairness. The company has never processed any data for other purposes, irrelevant or exceeding the activities necessary to provide the contracted service with its Customers ";

"No data relating to the reports has been disclosed or otherwise made accessible externally, nor to the internal staff of the company", having limited their activities to certain operations, such as, in particular, "the automatic system maintenance to guarantee the server up "and" application updates in the event of regulatory changes ";

"The assumption that the absence of the appointment pursuant to art. 28 GDPR automatically entails for CLIO having operated the processing of personal data in violation of art. 5 and in the absence of the conditions of lawfulness provided for in art. 6 of the Regulation, neither on a substantive level but not even on a formal one. The appointment does not represent the only legitimate basis for the processing of data, if the same are treated in accordance with the provisions of the Regulation and other laws that regulate a specific matter, as is the case in this case the discipline on Whistleblowing which is it is based precisely on the assumptions of confidentiality and data security […] Also ANAC within the 2021 guidelines reports verbatim on pages 6-7 "... 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 (Article 6, § 1, letter c) of the Regulation ), and, with regard to particular categories of data (art.9, § 2, lett.b) of the Regulation in relation to art. 54-bis) or data relating to criminal convictions and offenses, may also be considered necessary for the performance of a task of public interest contemplated by the law (art. 6, § 1, letter e) and art. 9, § 2, lett. g) and 10 of the Regulation) "".

"[After the inspection activity of the Guarantor] there have been copious regulatory interventions, opinions, consultations, guidelines (for example, the first opinion of the Privacy Guarantor to ANAC is of 4 December 2019) on the issues of Privacy and Whistleblowing which demonstrate how to bring the regulatory principles into the operational reality of Bodies and

suppliers is not a simple process, but requires clarification and support interventions in relation to the obligations and procedures to be adopted in order to correctly implement the regulations ";

"The treatment register has been duly populated";

"Following the inspection, [the Company] took steps to identify critical issues and improve company procedures with a view to correct compliance with the regulatory provisions both from a formal and substantive point of view".

Although the Company had expressly requested to participate in the hearing with the Authority, pursuant to art. 166, paragraph 6, of the Code, it is acknowledged that the same subsequently renounced being audited, recalling, with a specific note, the considerations already expressed in its defense writings (see note XX, in documents).

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 whistleblowing systems, due to its implications for the protection of personal data, has been under the attention of the supervisory authorities for some time. .it, web doc. no. 1693019; see, also, Working Group Art. 29, "Opinion 1/2006 on the application of EU data protection legislation to internal procedures for reporting irregularities concerning the keeping of accounting, internal accounting controls, auditing, the fight against corruption, banking and financial crime ", adopted on 1 February 2006, web doc. no. 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 they 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.

of European delegation 2021, 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 context, the processing of personal data carried out by subjects, public and private, required to comply with the aforementioned legal framework - which contains "more specific rules to ensure the protection of rights and freedoms with regard to the processing of personal data of employees in 'scope of employment relationships ”provided for by art. 88, par. 1, of the Regulation - can be considered necessary to fulfill a legal obligation to which the data controller is subject (art. 6, par. 1, lett. C), 9, par. 2, lett. b), and 10 of the Regulation).

In this context, the data controller, 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), may in any case resort to a data controller for the performance of certain processing activities, to whom it gives specific instructions (cons. 81, articles 4, point 8), and 28 of the Regulation) and must define its own reporting management model in compliance with the principles of "data protection by design" and "protection by default" (Article 25 of the Regulation), also taking into account the observations presented in this regard by the data protection officer (DPO).

3.1. Lawfulness of the processing carried out by the company providing the whistleblowing application.

For the purposes of compliance with the legislation on the protection of personal data, it is necessary, first of all, to precisely

identify the subjects who, for various reasons, can process personal data and clearly define their respective powers, in particular that of owner and manager. of the processing and of the subjects who operate under their direct responsibility (Article 4, points 7 and 8, 28 and 29 of the Regulation).

As clarified on numerous occasions by the Guarantor, the subjects obliged to comply with the aforementioned provisions must process the data necessary for the acquisition and management of the reports also in compliance with the regulations on the protection of personal data (see, on this point, provisions 10 June 2021, nos. 235 and 236, web doc. 9685922 and 9685947, 7 April 2022, nos. 134 and 135, web doc. 9768363 and 9768387).

In fact, these subjects, data controllers, fall within the decisions about the purposes and methods of processing the personal data of the interested parties, having in any case a "general responsibility" on the treatments put in place even when certain processing operations are carried out. by a data processor on their behalf, on the basis of the instructions given by the data controllers (cons. 79 and 81, art. 5, par. 2, which formalizes the so-called principle of "accountability", 24 and 28 of the Regulation; cf. 43, web doc. pursuant to the GDPR ", adopted by the European Data Protection Committee on 7 July 2021, spec. par. 174).

The owner can therefore entrust the performance of some processing activities to a manager - who presents sufficient guarantees on the implementation of technical and organizational measures suitable to ensure that the processing complies with the regulations on the protection of personal data (see cons . 81 and art.28, par. 1, of the Regulation) - governing the related relationship with a contract or other legal act and giving instructions on the main aspects of the processing, in particular, for the profiles of interest in the case question, "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 Regulation also governs the other specific obligations and other forms of cooperation to which the data controller is required and the scope of the responsibilities incumbent on the owner and manager respectively (see articles 30, 32, 33, par. 2, 82 and 83 of the Regulation).

In this context, therefore, the data controller is, in any case, 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), having to assist the latter in ensuring compliance with the obligations deriving from the data protection regulations, "taking into account the nature of the processing" and the specific legal regime applicable to the same (Article 28, paragraph 3, letter f), of the Regulation) .

With regard to the present case, it is therefore noted that the decision to make use of the services offered by an external company, rather than autonomously creating an application for the acquisition and management of reports of offenses, derives from a precise choice of the data controller which processes personal data in this context to fulfill a legal obligation deriving from the aforementioned regulatory framework on whistleblowing.

Although the Company has declared that no data relating to the reports has been made accessible not even "to the internal staff of the company", having limited itself, in providing the application in question, to carrying out certain operations, such as, in particular, "system maintenance automatic to ensure server back-up "and" application updates in the event of regulatory changes ", it is noted that the information contained in the reports of illegal conduct acquired through the application in question, in any case" installed on a server at the Company's data center ", even if subject to encryption, must be considered as personal data. In fact, data encryption constitutes an effective measure that the owner and manager, also based on the principles of data protection by design and by default, can adopt to make personal data incomprehensible to anyone not authorized to access - guaranteeing the security of the processing and protecting the rights and freedoms of the interested parties - but is not in itself suitable to make the encrypted information no longer referable to an identified or identifiable person (see cons. 83, and art. 4, point 1), 25 and 32, par. 1, lett. a), of the Regulations, see, lastly, provision 7 April 2022, n. 135, doc. web n. 9768387).

Therefore, the functions performed by the Company involved the processing of the personal data of the whistleblowers and other interested parties indicated in the reports (reported subjects, witnesses, etc.), of which each of its customers is in any case the owner, treating them on the basis of a specific obligation of law.

In such cases, the data protection regulations, as mentioned, 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 in the absence of a suitable prerequisite of lawfulness, given the notion of "third party" referred to in art. 4, point 10, of the Regulations; cf. art. 2-ter, paragraphs 1 and 4, lett. a) of the Code, which defines the "communication" of personal data.

Nevertheless, with regard to the present case, the relationship between some customers (Municipality of Ginosa and Acqua Novara.VCO S.p.a.) and the Company has not been regulated in terms of data protection, pursuant to art. 28 of the Regulation.

To the objections formulated by the Guarantor, the Company replied that, with regard to relations with the aforementioned customers, "no adaptation to art. 28 of the Regulations with a "formal" investiture by CLIO as Data Processor on the sidelines of the Supply Contract "but that in concrete terms this contract" implied de facto such a role on the part of the supplier ". In this regard, it is reiterated that, on the basis of the data protection regulations, when using a manager to carry out certain processing activities, the owner entrusts the tasks analytically specified in writing to the manager and also monitors their compliance.

The manager, in turn, carries out these treatments by following the instructions given by the owner and can, therefore, legitimately process personal data on behalf of the owner only on the assumption of a contract or other legal act, the existence of which does not constitute, contrary to what supported by the Company, a mere formal fulfillment, as it must regulate some of the most important aspects of the processing and implement the specific instructions of the owner. It follows that, more generally, the processing can in any case legitimately take place by the manager, only in the presence of suitable regulation of the relationship in terms of data protection and within the limits and in the manner dictated by the owner for the execution of data processing (see Article 28, paragraph 5, of the Regulation).

These principles were also applied with regard to the legal framework prior to the Regulation, as specified by the Court of Cassation (see Cass., Section I Civ., Ordinance no. 21234 of 23 July 2021, albeit in relation to the processing of personal data in a different context). In confirming a provision of the Guarantor, the Court, for the profiles that are relevant in the present case, specified that "the agreement between the" owner "and the" responsible "is legally required and is not intended only to regulate relations inter partes, with a purely internal value, from the point of view of any breach of contract - as the applicant erroneously claims -, because the discipline dictated therein by the "owner", regarding the purposes and methods of processing, becomes a necessary element for the qualification of "responsible" in the specific case ".

As previously clarified by the Guarantor with regard to similar cases, not having been identified as the data controller and not having been indicated by the Company specific conditions that have legitimized the processing of personal data, it must be concluded that the same has been carried out in the absence of the conditions of lawfulness provided for by the Regulations and the Code. Art. 6, par. 1, lett. c), of the Regulation, in fact, admits the processing if necessary "to fulfill a legal obligation to which the data controller is subject" and legitimizes the data controller, who is required to comply with the obligation, to process the data for this purpose. and not other subjects who process the data on behalf of the owner (on this point, with

regard to the lack of legitimacy of the treatment for the subjects who process the data on behalf and in the interest of the data controller, in case of failure to regulate the relationship to pursuant to art.28 of the Regulation, see provision 17 September 2020, nos. 160 and 161, web doc. n. 9461168 and 9461321; see also provision 11 February 2021, n. 49, web doc. 9562852, provision 17 December 2020, nn. 280, 281 and 282, web document n. 9524175, 9525315 and 9525337, as well as provision 10 February 2022, nn. 43 and 44, web document n. 9751498).

In light of the foregoing considerations, in the case in question, since the Company has not been identified as the data processor, in the absence of the required "documented instruction" by the owner (Article 28, paragraph 3, letter a), of the Regulation), and since no specific and autonomous conditions of lawfulness have been found to legitimize the processing of personal data by the same, it must be concluded that the processing of personal data contained in the reports of alleged offenses acquired through the aforementioned application was carried out in absence of the conditions of lawfulness provided for by the Regulations and the Code, in violation of articles 5, par. 1, lett. a), and 6 of the Regulations and art. 2-ter of the Code.

While taking into consideration the fact that, following the inspection activities, the Company has taken steps to solicit its customers in order to obtain the regulation of the related relationships from the point of view of data protection, it is believed that this circumstance cannot be considered sufficient for purposes of the exclusion of the Company's responsibility regarding the processing of personal data, prior to the regulation of such treatments pursuant to art. 28 of the Regulation.

3.2. Failure to keep the register of processing activities carried out on behalf of the data controllers.

The Regulation provides, among the general obligations connected to the processing of personal data, also the one, borne by each data controller and data processor (for the activities carried out on behalf of the data controller), to draw up "registers of processing activities "(Article 30 of the Regulation).

These registers, suitable for providing an updated picture of the treatments in place within your organization and / or the treatments carried out on behalf of the data controller, are essential to allow you to evaluate and document the compliance of the treatments with the rules on protection. of personal data and therefore are preliminary with respect to the start of the same (see on this point, provision of 7 April 2022, no. 134, web doc. no. 9768363, cit.).

With regard to the present case, it was ascertained that the register of the processing activities carried out on behalf of its customers, data controllers, was not kept in the context of the management of the application for the acquisition and

management of reports of illegal conduct , in violation of art. 30, par. 2, of the Regulation.

For these reasons, it must be considered that, up to the preparation of the aforementioned register, the Company has not fulfilled the obligation pursuant to art. 30, par. 2, of the Regulation.

4. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the Company 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.

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 consideration the provisions in force at the time of the violation committed, which - given the permanent nature of the alleged offenses - must be identified at the time of termination of the conduct. 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 by the Company in the absence of an appropriate legal basis is found, in violation of Articles 5 and 6 of the Regulations and art. 2-ter of the Code, and without keeping the register of processing activities carried out on behalf of the data controllers, in violation of art. 30, par. 2, of the Regulation.

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 Regulations and art. 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 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 its customers, 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 the Company provided extensive cooperation during the investigation, urging its customers to settle the related relationship pursuant to art. 28 of the Regulation and adopting measures aimed at ensuring that, also with regard to future customers, the correct definition of roles and responsibilities in the processing of data is always guaranteed, as well as preparing the register of processing activities carried out on behalf of its customers, holders of the treatment, and finally the financial statements were considered. Furthermore, there are no previous violations committed by the Company or previous provisions pursuant to art. 58 of the Regulation.

On the basis of the aforementioned elements, assessed as a whole, the amount of the pecuniary sanction is determined, in the amount of € 10,000.00 (ten thousand) for the violation of Articles 5, 6 and 30 of the Regulation as well as 2-ter of the Code, 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 reporting persons 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 Clio s.r.l. for the violation of articles 5, 6 and 30 of the Regulations as well as art. 2-ter of the Code in the terms set out in the motivation;

ORDER

a Clio s.r.l., in the person of the pro-tempore legal representative, with registered office in via 95 ° Regimento Fanteria 70, 73100 Lecce, Tax Code / VAT number 02734350750, pursuant to art. 58, par. 2, lett. i), and 83, par. 5, of the Regulations, to pay the sum of € 10,000.00 (ten 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 Clio s.r.l. to pay the sum of € 10,000.00 (ten 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, 21 July 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei