[doc. web no. 9891673]

Provision of April 13, 2023

Register of measures

no. 127 of 13 April 2023

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter, the "Regulation");

HAVING REGARD TO the Code regarding the protection of personal data, containing provisions for the adaptation of the national legal system to Regulation (EU) 2016/679 (legislative decree 30 June 2003, n. 196, as amended by legislative decree 10 August 2018, n. 101, hereinafter "Code");

CONSIDERING the complaint presented pursuant to art. 77 of the Regulation by prof. XX against SWG S.p.A.;

HAVING EXAMINED the documentation in the deeds;

HAVING REGARD TO the observations made by the general secretary pursuant to art. 15 of the Guarantor's regulation n. 1/2000;

SPEAKER Dr. Agostino Ghiglia;

WHEREAS

1. The complaint against the company and the preliminary investigation.

With a complaint dated July 22, 2020, Prof. XX complained about alleged violations of the Regulation by SWG S.p.A. (hereinafter, the Company), with reference to the replacement of the access credentials to the individualized e-mail account, assigned to the complainant, in the context of a plurality of coordinated and continuous collaboration relationships stipulated with the Company (XX@ swg.it) and the deactivation of the company telephone arranged, before the agreed termination of the employment relationship with the interested party, with the consequent complained impossibility, for the complainant, to access their personal data, even of a private and particular nature (Article 9 of the Regulation), contained in the account.

In this regard, the complainant asked the Company (on 17/7/2020) to "immediately unblock the company email", providing new

login credentials.

In responding to the request for information, the Company, with a note dated April 26, 2021, stated that:

to. "on 3 July 2020 [...] the Complainant [...] communicated via PEC to [...] the President of SWG, his intention to terminate the collaboration agreement with effect from 1 September 2020" (note 26/4/2021, pp. 4-5);

b. the Company "therefore reached an agreement for the consensual termination of the collaboration contract [...], with early effect from 31 July 2020, sent by SWG on 10 July 2020 by certified e-mail and subsequently signed by the [complainant] on 11 July 2020" (cited note, p. 5);

c. "as part of a technical verification scheduled for July 2020 and aimed at ensuring the correct transmigration of data following the logistical transfer of the Company's headquarters, on the evening of 10 July 2020, the system administrator [...] noted a series of unusual accesses to the corporate VPN on 3 July 2020. After some checks [...] it emerged that, exactly in the hour that preceded the sending of the PEC communication for the termination of the relationship, a massive download had been carried out, unusual and unjustified, of more than 600 files from the company's servers [...] from a single account" found to be the one assigned to the complainant (note cit., p. 5);

d. in order to "protect its legitimate and prevailing interest in the protection of the company assets" the Company has "arranged [the] blocking of the company e-mail box and SIM [...]" (note cit., p. 6);

And. "on 11 July 2020 the [complainant] contacted the [president of the Company] by telephone for clarification on the point, who represented [...] how the blocking of access had been ordered due to the ascertained multiple illegal conduct of the now former Collaborator" (cited note, p. 6);

f. "no prejudice was caused to the [complainant] who, in fact, should never have stored their personal data, even of a particular nature, with the aforementioned users" (note cit., p. 8);

g. according to the internal regulation on the use of IT devices, c.d. "Normative Document DN02", it was announced that "The mailbox, assigned by the Company to the user, is a work tool. […] It is forbidden to use one's company e-mail boxes to send personal messages"; furthermore "The non-compliance or violation of the rules contained in this regulation can be prosecuted with disciplinary measures" (note cit., p. 8 and Annex 10);

h. the complainant was informed of the content of the internal regulation "i) on the occasion of his appointment as data processor, which took place since the previous contract relating to the 2015-2017 period (Annex 11) and ii) on the occasion of

the training events on the management system quality dated 13 April 2015, 9 November 2017 and 15 January 2020 (Annex 12)"; moreover, the Company "has [...] taken steps [...] to inform its collaborator on the purposes and methods of processing their personal data, pursuant to and for the effects of the legislation in force at the time of signing the collaboration contract" (note cit. , p. 9);

the. currently "the account is not active, as it was deactivated at the same time as the detection of multiple abusive accesses" (note cit., p. 10);

j. the reasons for which the Company has inhibited access to the company account reside "in the containment of a security incident which resulted in the withdrawal of confidential documents and information (as many as 600 files)" (note cit., p. 10);

k. the activities subsequent to the "detection of unauthorized access [...], by the system administrator" are contemplated "by the specific privacy and data security management procedure adopted by SWG (Annex 13), also communicated to the [complainant] i) on the occasion of his appointment as data processor (Annex 11) and ii) on the occasion of the training events on the quality management system of 13 April 2015, 9 November 2017 and 15 January 2020 (Annex 12)" (note cit., p. 10-11);

L. "Currently no communication relating to the company mailbox of the [complainant] is held on company servers, except for the related backup" (note cit., p. 11);

m. "the system administrator [...] i) on 10 July 2020 changed the passwords relating to the company email account of the [complainant]; ii) on 11 July 2020 he contacted the company's telephone operator in order to request the blocking of the company SIM as well, which was completed approximately two days after the request; iii) when the employment relationship was terminated, the user was deactivated and the appropriate automatic message entered" (cited note, p. 12);

no. "In the present case, the deactivation was prior (only) 15 days to the formal termination of the employment relationship due to the ascertained unlawful conduct committed by the person concerned" (note cit., p. 13);

or. "the refusal to request access to the Collaborator's company user occurred in the face of [...] legitimate interest of SWG, of a prevailing nature with respect to the rights and freedoms of the [complainant], pursuant to art. 6, par. 1, lit. f), GDPR" (note cit., p. 13);

p. "the Collaborator's access to his corporate user would have further exposed - perhaps irreversibly - the Company to further damages, consisting precisely in the theft of confidential information and, therefore, corporate secrets" (note cit., p. 15);

q. with reference to the request to access the account formulated by the complainant "upon receipt of the certified e-mail dated

13 July 2020, already the following day (14 July 2020) [the lawyer who acted in the name and on behalf of the Company], in contesting unlawful conduct was detected, proceeded to communicate [...] the refusal of access, arguing that it resided precisely in the guarantee of the company's assets and in the defense of the rights of the owner in court. In fact, as provided for by art. 15 GDPR, fourth paragraph, the right in question must not harm the rights and freedoms of others, without prejudice to what has already been reported on the provision of Recital 63 GDPR, of explicit protection of industrial and corporate secrets and intellectual property" (note cit., p 17).

With counter-arguments of 8/11/2021, the complainant represented that:

to. "at the date of the alleged offenses committed by the complainant, the contract stipulated by the parties on 18 December 2018 was still in force" (note 1/8/2021, p. 4);

b. "on 11 July 2020, the parties formalized the verbal agreements by ratifying the termination of the existing relationship and "reciprocally confirming their willingness to consensually terminate the collaboration agreement with effect from 31 July 2020"" (note cit., p. 4) ;

c. "the downloading of the data took place in the context of the contractual relationship and therefore is anything but abusive" (note cit., p. 4);

d. "it is not possible to understand why the account access credentials were blocked [...] and not just access to the company server [...] the same applies to the blocking of the company mobile phone" (note cit., p. 4) ;

And. the document called DN02, "whose date of formation is uncertain", was never delivered or in any case made known to the complainant (note cit., p. 6);

f. with regard to training events "these events do not indicate specific training in the field of data protection and processing and/or use of information systems [...] Moreover [...] no proof is provided as to the effective participation [of the complainant] in such events" (note cit., p. 7);

g. "the alleged exercise of a right of defense in court [...] is irrelevant since the mitigation of information obligations [...] does not affect the obligation of the controller to indicate, in advance and in a transparent manner, the control activities that can be carried out" (note cit., p. 8);

h. it does not emerge from any document that the complainant had the obligation "not to include information of a personal nature on his email or on his SIM card" (note cit., p. 11);

With subsequent briefs dated October 18, 2021, the Company replied that:

to. as claimed by the complainant, the action of changing the server access password would not have been sufficient, given that the Company in this way could not have "protected the information object of the massive download except by preventing its diffusion by blocking the users and the simultaneous recovery of the devices" and therefore "the access of the [complainant] to his corporate user would have exposed the company to further damages, consisting precisely in the theft of confidential information" (note 10/18/2021, p. 3) ;

b. the regulation on the use of IT devices was "made known" to the complainant "on the occasion of his appointment as person in charge of processing" and "on the occasion of information events on the quality management system"; in this regard it is also specified that "the document produced in the deeds [...] constitutes [...] digital copy of the Regulations, as such does not require the signature of the collaborator [...]" (note cit., p. 5-6);

c. "the assessment of suspicious traffic during the data transmigration check integrates the scenario contemplated by the specific privacy and data security management procedure adopted by SWG (Annex 13), also communicated to the [complainant]" (note cit., p. 7);

d. with reference to the blocking of the company users of the complainant, ordered by the Company, "the remedy to be undertaken should not have concerned so much the migration from the server to the local device (by now held and concluded, in the seven days prior to the discovery event) but that of diffusion" (note cit., p. 7-8);

And. on the corporate Intranet "all the procedures implemented by the company are placed and updated" (note cit., p. 8).

With the additional note dated 18 March 2022, sent in response to the request for further clarifications by the Office (dated 28/2/2022), the Company stated that:

to. as regards the concrete procedure adopted by the system administrator, in view of the transfer of the head office, the Company "has prepared a complete migration plan [...]. In particular, the plan included switching off, moving and restarting the Network Attached Storage [...]. Based on the objectives described above, on Friday 10 July 2020 [the system administrator] proceeded to analyze the traffic generated [...]. On that occasion, [the administrator] detected an anomaly, namely that an important number of files had been opened for reading on Friday 3 July 2020: considering that, from the examination of the logs of the previous weeks and months, an estimated average activity on a few files per day or week by collaborators, this event was completely anomalous and as such suspicious" (note 18/3/2022, p. 2);

b. in response to this detection, the system administrator "immediately applied the privacy and data security management procedure adopted by SWG (Annex 13)" (note cit., p. 2-3);

c. subsequently the system administrator "therefore: [...] reported the situation to the Company [...]; suspended the user that generated the event, for the purpose of further investigation and awaiting indications from the company; definitively suspended the user following the indications of the Company" (note cit., p. 3);

d. by letter dated November 27, 2020, a technical consultant was appointed to carry out the forensic copy, indexing and analysis of the notebook assigned to the complainant; the consultant's technical report had been delivered to the Company on 18 December 2020 (note cit., pp. 4-5).

2. The initiation of the procedure for the adoption of corrective measures and the deductions of the Company.

On 2 May 2022, the Office carried out, pursuant to art. 166, paragraph 5, of the Code, the notification to the Company of the alleged violations of the Regulation found, with reference to articles 5, par. 1, lit. a) and 13 of the Regulation.

With defense briefs sent on 1 June 2022, the Company represented that:

to. has not carried out and does not carry out "preventive and continuous checks on the use of company tools"; "the only type of «control» contemplated by the [internal] Regulation was, in fact, that aimed at verifying and contrasting «those incorrect uses which, in addition to exposing the company to both financial and criminal risks, can in themselves consider themselves contrary to the duties of diligence and loyalty [...] (see point 6 of the Regulation), [...]. This aspect was brought to the attention of employees and collaborators" (see memorandum of 1/6/2022, p. 9);

b. "the verification activities carried out [by the Company] constituted an exception, amply motivated by the need to ascertain and counter malicious conduct - after it has occurred - [...], and in any case contemplated by company procedures" (see memorandum cited, p. 10);

c. "the assessment activity carried out [...] on the evening of 10 July 2020 was carried out on the occasion of another scheduled activity of the system administrator [...] which in itself would not have involved any processing of personal data except for following the detection of an anomaly of an exceptional nature, consisting of a massive download of confidential company data that could not be [...] ignored" (see the aforementioned brief, p. 10);

d. "a total absence of information nor inadequate information from the collaborator does not appear to be identifiable", given that, as already declared during the proceedings, information in this regard was provided on the occasion of the appointment

as person in charge of processing and during the training events (see memorandum cited, p. 12);

And. if the Authority decides to confirm the ascertainment of the violation of art. 13 of the Regulation, it should be taken into account that the Company's activity "was carried out solely for the purpose of protecting its rights in court, both in civil and criminal matters, by carrying out [...] defensive investigation activities foreseen and regulated in the code of criminal procedure" (taking into account the provisions of article 23 of the Regulation and article 11 of the ethical rules relating to the processing of personal data carried out to carry out defensive investigations or to assert or defend a right in court judicial; see memorandum cited., p. 13);

f. following the conclusion of the relationship with the complainant, the Company, as part of a broad compliance activity regarding the processing of personal data of employees and collaborators, updated the information documents prepared pursuant to articles 13 and 14 of the Regulation and the regulation relating to the use of company tools; moreover, the Company has activated improvement actions in the field of cybersecurity, in particular with the release of a new VPN system and the "change to the configuration of the file server [...] to obtain greater granularity in the definition of read permissions, currently segmented by individual order" (see memorandum cited, p. 15);

g. finally, the Company has provided all the elements referred to in art. 83, par. 2 of the Regulation.

During the hearing, held on 26 July 2022, the Company finally declared that:

to. some proceedings are currently pending against the complainant before the ordinary judicial authority, activated by the Company for his protection;

b. the verification activity on the information systems made it possible to ascertain that the files involved "concerned various orders in progress and which covered an extended time interval from 2014 to 2020. [...] It involved the downloading of an entire database with information business confidentiality (not personal data)";

c. "no unlawful conduct by the Company can be identified, given that the check took place only once, with an urgent nature to deal with a substantial anomaly (i) after it occurred, (ii) with reference to a single collaborator, (iii) to defend the corporate assets and the legitimate interest of SWG";

d. "during the checks carried out, the system administrator ascertained the presence of an anomaly, but not a data breach as the stolen information did not contain personal data. This is because, in application of the principle of privacy by design, the system allowed access to the data on the basis of the different granularity of the permits, in particular the complainant did not

have access to data that were not aggregated".

3. The outcome of the investigation and of the procedure for the adoption of corrective and sanctioning measures.

3.1. Outcome of the investigation.

As a result of the examination of the declarations made to the Authority, during the proceeding as well as of the documentation acquired, it appears that the Company, as owner, has carried out some processing operations, referring to the complainant, which are not compliant with the regulations in matter of personal data protection.

In this regard, it should be noted that, unless the fact constitutes a more serious offence, anyone who, in a proceeding before the Guarantor, falsely declares or attests news or circumstances or produces false deeds or documents, is liable pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the performance of the duties or exercise of the powers of the Guarantor".

On the merits, it emerged that the system administrator, as part of the activities aimed at the efficient management of the migration of systems on the occasion of the transfer of the Company's headquarters, on 10 July 2020, analyzing the traffic generated, found "a anomaly i.e. that an important number of files had been opened for reading on Friday 3 July 2020".

Having detected the anomaly, the system administrator carried out further checks, ascertaining that: the user concerned was that of the complainant; the accesses "had been carried out "in reading" and concerned a considerable amount of different files, taken from shared folders"; in the light of "[t]he time of downloading files, close and sequential" it had to be concluded "that the activity had been of massive copying".

At this point, the system administrator notified the Company and, at the same time, temporarily suspended the complainant's utilities, pending further instructions, upon receipt of which the aforementioned utilities were definitively suspended.

The system administrator, once ascertained an anomaly that could have been an indication of an ongoing danger to the safety of the systems, then proceeded to carry out investigations which led to the identification of a user (the complainant) of the same systems , the precautionary suspension of the account and the subsequent definitive blocking of the e-mail box and SIM.

At the end of the proceeding, it also emerged, with regard to the alleged violation of the complainant's right to access the account, that the request (contained in the formal notice dated 17/7/2020) actually had as object the communication of new access credentials and that the Company had already represented to the interested party (with a note dated 14/7/2020) that in the presence of specific needs for the protection of one's rights, which emerged after the discovery of suspected illegal

activities by the complainant, it would not have been possible to reinstate the complainant in access to the e-mail box.

With regard to the proceedings pending before the ordinary judicial authority between the same parties to the present proceedings, in relation to various profiles, of which some extracts and a copy of a provision have been produced in the documents, it is recalled that pursuant to art. 160-bis of the Code "The validity, effectiveness and usability in judicial proceedings of deeds, documents and provisions based on the processing of personal data that does not comply with the provisions of the law or the Regulations remain governed by the pertinent procedural provisions".

3.2. Violation of articles 5, par. 1, lit. a) and 13 of the Regulation.

In relation to the described activity carried out following the detection of an "anomaly" by the system administrator, at a time when the user/complainant was still entitled to carry out the operations ordinarily permitted for the performance of the professional activity (given that an agreement between the Company and the interested party for the early termination of the contract was agreed only on the same day, which would in any case have taken effect at the end of the month), it is ascertained that the Company has failed to inform the complainant about the possibility, for the latter, to carry out surveys on the contents stored on company devices (notebooks and smartphones), as well as to analyze the activities carried out through the devices themselves, identifying, even after a gradual survey, the single user of a user to which activities deemed "anomalous" are connected.

In fact, the internal regulation on the use of IT devices, the so-called "Normative Document DN02", version of 1 October 2018 (Annex 10, note SWG 26.4.2021), does not contain any reference to the possibility of carrying out checks aimed at verifying compliance with the rules ("It is forbidden to use the company e-mail boxes for sending personal messages") contained in the document itself, given that such cannot be considered the notice that "failure to comply with or breach the rules contained in this regulation can be prosecuted with disciplinary measures as well as with civil and criminal actions allowed" (point 9), since it is exclusively an indication of the consequences of any violation of company rules.

Not even the "Document DN01 - Management of Privacy and Data Security", version of 1 October 2018 (Annex 13, note SWG 26.4.2021), contains specific information elements regarding the type of controls on corporate instruments that the Company reserves the right to carry out, much less attributable to those actually carried out in the case in question (collection of data relating to "anomalous" activities, identification of the single workstation, examination of the data contained in the returned company devices).

In fact, point 4.2 of this document ("IT data security management") contains an indication of the security measures adopted (divided into: "Data server situation"; "USERNAMES and PASSWORDS management"; "Protection against intrusions from software" ["computer viruses"]), while point 6 (Company regulation for the use of computer systems) represents in principle the need to "put in place adequate control systems on the use [of the computer tools provided by the 'company] by collaborators" without however indicating them.

Nor the subsequent reference to "preventive and continuous controls on the use of IT tools [which] must guarantee both the employer's right to protect his organization [...] and the worker's right not to see his personal sphere invaded, and therefore the right to confidentiality and dignity as sanctioned by the Articles of Association and by the Privacy Code" allows for detailed information on the proposed verification activities, especially since the paragraph closes with a reference to the aforementioned Regulatory Document DN02 ("in order to reconcile the aforementioned needs"), which, as already noted above, does not contain information on possible control activities on the use of the devices.

Having acknowledged that the Company has declared in its defense briefs that, despite the vagueness of the formulation referred to above, it does not carry out and has not carried out "preventive and continuous checks on the use of company tools", the verification activity carried out by the director of system consisted precisely in the "verification and [...] contrast of «those incorrect uses which, in addition to exposing the company to financial and criminal risks, can in themselves be considered contrary to the duties of diligence and loyalty [...]"" (see defense briefs, p. 9), without, however, the interested party having been informed in advance of the purposes and methods of the proposed controls as well as the consequences of the same, also in terms of accessibility and deactivation of the company tools made available for the execution of work performance.

Furthermore, it does not appear that, at the time of the facts which are the subject of the complaint, there were active measures, even of a technological nature, aimed at preventing the activities contested by the complainant. In this regard, it is noted that, during the proceeding, the Company made some changes also in relation to the definition of reading permissions, based on greater granularity and "currently segmented by individual order".

Furthermore, during the proceeding, it did not emerge that suitable information elements were provided to the complainant at the time of stipulation of the contract or of the appointment as person in charge of processing or on the occasion of the performance of "training events on the quality management system" (which, moreover, it does not appear that the interested

party participated).

Finally, the reference to the c.d. "theory of defensive checks", of pure jurisprudential creation, carried out in the defense briefs, given that, in the present case, the Authority has not formulated observations regarding the sector discipline on remote checks (Article 114 of the Code).

The employer has the duty to indicate to its employees and collaborators, in any case, clearly and in detail, which are the methods of use of the tools made available that are considered correct and if, to what extent and with what modalities, even in the event of unforeseen or exceptional events, checks are carried out which must in any case comply with the principles of lawfulness, proportionality and gradualness (see Guidelines of the Guarantor for e-mail and internet, Provision 1/3/2007, n. 13 , in Official Journal no. 58 of 10/3/2007, web doc. no. 1387522).

In the context of the employment relationship, regardless of the nature of the latter, the obligation to inform the interested parties about the treatments carried out or which we reserve the right to carry out also constitutes an expression of the general principle of correctness (Article 5, paragraph 1 , letter a) of the Regulation).

The Company, in the case subject to the complaint, has therefore failed to inform the complainant about the specific treatment method actually carried out through the checks carried out on the use of IT devices and the analysis of the data contained within its devices subject to redelivery (subsequently subjected to forensic investigation activities), in violation of the provisions of art. 13 of the Regulation as well as art. 5, par. 1, lit. a) of the Regulation which establishes the general principle of correctness of processing.

With reference to the information documents prepared during the proceedings (bearing the date 05/26/2022), attached to the defense briefs of June 1, 2022 (Information pursuant to Article 13 of the GDPR for collaborators; Information pursuant to Article 13 of the GDPR for employees; Disclosure pursuant to Article 4, paragraph 3 of the Labor Code and Article 13 of the GDPR for employees; Regulations for the use of company tools and on the checks carried out by the employer in relation to their correct use), the Company is invited, pursuant to of the art. 57, par. 1, lit. d) of the Regulation, to take into account the provisions of the Authority regarding the processing of data relating to employees' e-mail and web browsing, also with regard to the application of the regulations on remote controls and the prohibition of investigations on the opinions referred to in Articles 114 and 113 of the Code (in relation to art. 88 of the Regulation), most recently with the provisions of 1 December 2022, n. 409 (web doc. n. 9833530), 13 May 2021, n. 190 (web doc. n. 9669974) and 15 April 2021, n. 137 (web document n. 9670738).

4. Conclusions: declaration of illegality of the treatment. Corrective measures pursuant to art. 58, par. 2, Regulation.

For the aforementioned reasons, the Authority believes that the declarations, documentation and reconstructions provided by the data controller during the preliminary investigation do not allow the findings notified by the Office to be overcome with the act of initiating the procedure and that they are therefore unsuitable to allow the filing of this proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

The processing of personal data carried out by the Company and in particular the carrying out of checks and controls on the activities carried out using company devices is in fact illegal, in the terms set out above, in relation to articles 5, par. 1, lit. a) and 13 of the Regulation.

The violation ascertained in the terms set out in the reasoning cannot be considered "minor", taking into account the nature and seriousness of the violation itself, the degree of responsibility, the manner in which the supervisory authority became aware of the violation (see Recital 148 of the Regulation).

Therefore, given the corrective powers attributed by art. 58, par. 2 of the Regulation, a pecuniary administrative sanction is ordered pursuant to art. 83 of the Regulation, commensurate with the circumstances of the specific case (Article 58, paragraph 2, letter i) of the Regulation).

5. Adoption of the injunction order for the application of the pecuniary administrative sanction and accessory sanctions (articles 58, paragraph 2, letter i), and 83 of the Regulation; art. 166, paragraph 7, of the Code).

At the end of the proceeding it appears that SWG S.p.A. has violated the articles 5, par. 1, lit. a) and 13 of the Regulation. For the violation of the aforementioned provisions, the application of the pecuniary administrative sanction envisaged by art. 83, par. 5, letter. a) and b) of the Regulation, through the adoption of an injunction order (art. 18, law 11.24.1981, n. 689).

Considering it necessary to apply paragraph 3 of the art. 83 of the Regulation where it provides that "If, in relation to the same treatment or related treatments, a data controller [...] violates, with willful misconduct or negligence, various provisions of this regulation, the total amount of the pecuniary administrative sanction does not exceed amount specified for the most serious violation", the total amount of the fine is calculated so as not to exceed the maximum prescribed by the same art. 83, par. 5.

With reference to the elements listed by art. 83, par. 2 of the Regulation for the purposes of applying the pecuniary administrative sanction and the relative quantification, taking into account that the sanction must "in any case [be] effective, proportionate and dissuasive" (Article 83, paragraph 1 of the Regulation), it is represented that In the present case, the

following circumstances were considered:

a) in relation to the nature and seriousness of the violation, the nature of the violation was considered relevant, which concerned the general principles of processing and the obligation to provide information (Article 83, paragraph 2, letter a) of the Regulation) ;

b) with regard to the degree of responsibility of the data controller, the conduct of the Company which did not comply with data protection regulations in the context of the employment relationship with its employees was taken into consideration; in this regard, as deduced in the defense briefs, the provisions of art. 23 of the Regulation in relation to art. 11 of the Ethical rules relating to the processing of personal data carried out to carry out defensive investigations or to assert or defend a right in court published pursuant to art. 20, paragraph 4, of Legislative Decree 10 August 2018, n. 101, considering that the disputed conduct was carried out before the assignment entrusted to the consultant in the context of a proceeding before the criminal judge (Article 83, paragraph 2, letter b) of the Regulation);

c) with regard to the degree of cooperation with the Supervisory Authority, it was considered that the Company has constantly cooperated with the Guarantor during the proceeding (Article 83, paragraph 2, letter f) of the Regulation);

d) in favor of the Company, the absence of previous violations regarding the protection of personal data and the small number of data subjects involved were taken into account (Article 83, paragraph 2, letters a) and e) of the Regulation).

It is also believed that they assume relevance in the present case, taking into account the aforementioned principles of effectiveness, proportionality and dissuasiveness with which the Authority must comply in determining the amount of the fine (Article 83, paragraph 1, of the Regulation), in firstly the economic conditions of the offender, determined on the basis of the revenues achieved by the Company with reference to the ordinary financial statements for the year 2021.

In the light of the elements indicated above and the assessments made, it is believed, in the present case, to apply against SWG S.p.A. the administrative sanction of the payment of a sum equal to 15,000 (fifteen thousand) euros.

In this context, it is also considered, in consideration of the type of violations ascertained that concerned the general principles of treatment and the obligation to provide information, that pursuant to art. 166, paragraph 7, of the Code and of the art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019, this provision must be published on the Guarantor's website.

It is also believed that the conditions pursuant to art. 17 of Regulation no. 1/2019.

ALL THAT BEING CONSIDERED, THE GUARANTOR

notes the illegality of the processing carried out by SWG S.p.A., in the person of its legal representative, with registered office in Via san Giorgio, 1, Trieste (TS), P.I. 00532540325, pursuant to art. 143 of the Code, for the violation of the articles 5, par. 1, lit. a) and 13 of the Regulation;

ORDER

pursuant to art. 58, par. 2, lit. i) of the Regulation to SWG S.p.A., to pay the sum of 15,000 (fifteen thousand) euros as an administrative fine for the violations indicated in this provision;

ENJOYS

then to the same Company to pay the aforementioned sum of 15,000 (fifteen thousand) euros, according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of adopting the consequent executive deeds pursuant to art. 27 of the law n. 689/1981. It should be remembered that the offender retains the right to settle the dispute by paying - always according to the methods indicated in the attachment - an amount equal to half of the fine imposed, within the term referred to in art. 10, paragraph 3, of Legislative Decree lgs. no. 150 of 09.01.2011 envisaged for the lodging of the appeal as indicated below (art. 166, paragraph 8, of the Code);

HAS

the publication of this provision on the Guarantor's website pursuant to art. 166, paragraph 7, of the Code and of the art. 16, paragraph 1, of the Guarantor Regulation n. 1/20129, and believes that the conditions pursuant to art. 17 of Regulation no. 1/2019.

Pursuant to art. 78 of the Regulation, as well as articles 152 of the Code and 10 of Legislative Decree no. 150/2011, opposition to the ordinary judicial authority may be lodged against this provision, with an appeal lodged with the ordinary court of the place identified in the same art. 10, within the term of thirty days from the date of communication of the measure itself, or sixty days if the appellant resides abroad.

Rome, 13 April 2023

PRESIDENT

station

THE SPEAKER

guille

THE SECRETARY GENERAL

Matthew