[doc. web n. 9751498]

Injunction order against the Tuscany Region - 10 February 2022

Record of measures

n. 43 of 10 February 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, Prof. Ginevra Cerrina Feroni, vice president, Avv. Guido Scorza, member, 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. The violation of personal data.

With a note of 30 July 2020 - integrated with the subsequent notes of 31 July and 6 August 2020 - the Tuscany Region notified

this Authority, pursuant to art. 33 of the Regulations, a violation of personal data, which took place on 27 July 2020. In particular, the accidental publication of some personal data was represented, referring to 3,548 interested parties, who participated, as candidates, in the pre-selection tests, held on the of 21, 22 and 23 July 2020, of the public competition for exams for the permanent recruitment of n. 84 administrative assistants, issued by executive decree no. 1076 of 24 January 2020.

In particular, the Tuscany Region highlighted that on 27 July 2020, at 3.45 pm, the person in charge of the aforementioned insolvency procedure received a report about the publication, within a group established on an instant messaging system (WhatsApp) and relating to the aforementioned competition, "of the screenshot of a communication apparently passed between a candidate and the company Scanshare S.r.l., entrusted with the organization and management service of the preselection of the competition tests and in charge of the processing of data relating to the pre-selection tests following the stipulation of contract". In said screenshot a web address was shown from which it was possible to download a file with the personal data of those who had participated in the pre-selection on 21, 22 and 23 July 2020 and the scores of the related tests. The image of a page of the file was also sent to the person in charge of the procedure and, subsequently, in the full version "also sent on the same whatsapp group" (see notification of 30 July 2020), who " immediately in contact with the contractor, in order to immediately suspend the unauthorized and non-agreed publication of the aforementioned data and information ".

The Region has represented that, "from what was reported by the Data Processor, during the upload phase of the data subject to the violation in order to prepare the files and documents to be sent to the administration [...], an email was erroneously sent to a candidate who asked, directly from the contractor, information regarding the timing of the publication of the results, containing the url that would host the portal for accessing candidates to their test and results and "pointing" to the uploaded web application, and therefore incomplete, from which it was possible to access the data in question. The violation occurred due to the random coincidence of the portal url with the path in which the data was being transmitted. This criticality, as reported by the data controller, lasted the time necessary for the data transfer to be completed. The upload started at 14:49 and ended at 15:49 "(see notification of 30 July 2020).

The Region also pointed out that, after becoming aware of the violation, "already starting at 3.45 pm on 27/07/2020 [... proceeded] to the formal challenge to the contractor for violation of the obligations assumed with the custody contract of the service of "Organization and management of the preselection of competition tests" CIG 815268507F, signed by the parties on

17/07/2020, in particular with reference to art. 16 "Personal data processing" of the aforementioned contract and art. 2 relating to the "Supplier's Obligations" of the special descriptive and performance specifications ", wary of Scanshare S.r.l. (hereinafter the Company) from "repeating or persevering in the aforementioned harmful and grossly negligent behaviors".

The Region also provided a copy of the report produced by the Company on 30 July 2020, in which, among other things, it is reported that “a request for the logs of the IP addresses that had access to the data was forwarded to Hostinger. It is presumed that a small number of candidates had access [and] it appears, from what was learned also from public facebook pages, that many participants in the pre-selection tests even after accidental access to the data did not have knowledge of the results "and that" the data accidentally published were contained in files and tables not easy to interpret ”.

With notes sent between 31 July and 17 September 2020, this Authority received numerous complaints (several dozen) relating to the issue described above and presented, also collectively, by the participants in the aforementioned competition, in relation to the profiles of competence in the field of protection. of personal data.

2. The preliminary activity.

With a note dated 9 September 2020, the Region, in response to requests for information made by the Office, stated, in particular, that:

“During the breach, the data was present on the system entirely managed by the Manager and located in a cloud system of his choice. In particular, the incident occurred during the data uploading phase on this system; at this stage no one should have had access to anything. During the data upload phase, the protection system was not configured and therefore the data was made available to anyone with the link. This link [("https://scanshareservice.com/regione-toscana/")] was erroneously provided by the helpdesk service of the Manager to a candidate, at the request of the latter, on 27/07/2020, before the date agreed for the authenticated publication, on the website of the Manager, of the results for each candidate. The Tuscany Region site reported, and still reports, only the link to this system ";

"It was in no way possible to access the documentation produced at the time of submitting the application as this is stored in a system, other than the one referred to, located by the Data Controller in the Cloud System of the Tuscany Region";

"After the performance of the pre-selection test, the transmission, by the Manager to the Data Controller, of the personal data of the candidates and the results of the test, took place by means of a communication via certified e-mail containing the results of the pre-selection test with the list of candidates admitted to the written test in addition to the results of the individual tests to

proceed on 27/07/2020 (protocol RT 0259786) in excel and pdf format, for the continuation of the administrative procedure starting from the list of candidates admitted to the next test ";

"The Region has appointed the Company, pursuant to art. 28 of the Regulations, responsible for the processing (as per the contract for the assignment of the "Organization and management of the preselection of competition tests" service) but has never "received communications or requests for authorization from [the same] regarding the involvement of third parties and their appointment as sub-data processors ".

With a subsequent note dated November 20, 2020, the Region also provided the Authority with the technical offer of the Company, entrusted with the organization and management service of the preselection of the competition tests, an integral part of the service award contract, in which it is specified that "Scanshare will guarantee, immediately after the completion of the tests, the online access of the documents, the personal data sheet, the matching code and the corrector to the Candidate who, with a username and password, will be able to view his / her document" (see annex 3 to the aforementioned note of 20 November 2020).

With a note dated 4 December 2020, the Office, on the basis of the elements acquired, the checks carried out and the facts that emerged as a result of the investigation, notified the Region of Tuscany, 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, concerning the alleged violations of articles 5, par. 1, lett. a), and 6, par. 1, lett. c) and e), of the Regulations and art. 2-ter of the Code (in the text prior to the amendments made by the legislative decree 8 October 2021, n.139, converted, with modifications, by the law 3 December 2021, n.205), inviting the aforementioned holder to produce defensive or documents or to ask to be heard by the Authority (art. 166, paragraphs 6 and 7, of the Code, as well as art. 18, paragraph 1, l. November 24, 1981, n. 689).

The Region sent its defense briefs with a note dated January 4, 2021, representing, among other things, that:

"Despite all the precautions taken by the Entity, the entrusted company was in any case responsible for the" Data breach "incident that occurred alongside the insolvency procedure, caused by a direct communication via email to a candidate, by a employee of the company "Scanshare", of the URL where, incidentally, the data referring to the candidates who participated in the pre-selection tests of the procedure in question were being uploaded ";

"Such direct communication [has never] been authorized by the Administration, being on the contrary provided in open violation of the contractual clauses [...]. Otherwise, in the special descriptive and performance specifications for the

procurement of the organization and management service of the pre-selection procedures it is envisaged that "Scanshare will guarantee, immediately after the conclusion of the tests, the online access of the documents, the personal data sheet, the matching code and the corrector to the Candidate who, with username and password, will be able to view his / her work "[...] precisely in order to ensure the security of access to authorized persons only";

the Region "as soon as it became aware of what happened, put in place an immediate and timely reaction, acting immediately, every instrument of denunciation and protection provided for by the current legislation, even with the aim of mitigating, as far as inherent to the own power of action, the negative consequences of the incident for all concerned ";

"As reported by the entrusted company responsible for the treatment, access to the environment in the phase of uploading the candidates' data occurred only by accidental direct communication of the URL for access to a single candidate - and it remains unproven to this day that such candidate has disclosed the access credentials to others. It is reasonable to state that tracing the URL through an ordinary "navigation" on the web in the time frame (in any case limited) of data upload was, if not impossible, so difficult as to assume the character of absolute improbability; however reasonable and known to the Writer, the exposure nevertheless produced only one unauthorized access, with all the consequent assessments in relation to the seriousness of the violation ";

"Already in the preparatory phase at the start of the selections, [the Region with] Article 16 of the service contract stipulated with the contractor company prescribes that" The contractor, as Manager, provides sufficient guarantees, in particular in terms of of specialized knowledge, reliability and resources, to implement technical and organizational measures that meet the regulatory requirements established by the GDPR, the Privacy Code and any other related standard concerning the processing of personal data, including processing security measures, to ensure the confidentiality and protection of the rights of data subjects. The contractor, as Manager, is required to ensure and ensure to its employees, collaborators and other managers, the confidentiality and correct treatment of information, documents and administrative acts, of which it becomes aware during the execution of the performance";

"The undersigned [...], following the knowledge of the violation, [has adopted] every useful measure to avoid its negative effects, in the first instance acting to guarantee the subjective position of the interested parties, [...] communicating to each of the over three thousand five hundred candidates, promptly, [...], the incident of the "data breach" occurred. In the second instance, also for the purpose of deterring further violations, it has already sent a warning to the responsible company

"Scanshare" on 29/07/2020 ";

"On 23/12/2020, the Tuscany Region sent a further warning to the contractor company, also in relation to the last dispute of this Authority of 03/12/2020, reserving any action for recourse if, at the outcome of this proceeding, it should a sanction be imposed on it ".

3. Outcome of the preliminary investigation.

3.1. The regulatory framework.

The rules on the protection of personal data provide that public subjects, even if they operate in the performance of insolvency, selective or otherwise evaluative procedures, preliminary to the establishment of the employment relationship, may process the personal data of the interested parties (Article 4, point 1) of the Regulation), if the processing is necessary "to fulfill a legal obligation to which the data controller is subject" (think of specific obligations under national legislation "for recruitment purposes", art. 6, par . 1, lett. C), 9, par. 2, lett. b), and 4, and 88 of the Regulation) or "for the performance of a task of public interest or connected to the exercise of public authority vested in the data controller" (Article 6, paragraph 1, lett e), of the Regulation).

European legislation provides that "Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing, in accordance with paragraph 1, letters c) and e), by determining more precisely specific requirements for processing and other measures aimed at guaranteeing lawful and correct processing […] "(Article 6, par. 2, of the Regulation). In this regard, it should be noted that the "dissemination" of personal data (such as online publication), by public entities, is permitted only when provided for by a law or, in the cases provided for by law, by regulation (art.2-ter of the Code, then amended by the aforementioned legislative decree no. 139 of 8 October 2021).

The data controller is then, in any case, required to comply with the principles of data protection, including that of "lawfulness, correctness and transparency", on the basis of which personal data must be "processed lawfully. , correct and transparent towards the interested party "(art. 5, par. 1, lett. a), of the Regulations).

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 no. 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).

3.2. Dissemination of personal data.

On a preliminary basis, it is acknowledged that the Region has promptly notified the violation of personal data to the Authority and has promptly informed, via an e-mail message, the interested parties involved in the violation, in accordance with art. 33 and 34 of the Regulations, also adopting measures - which the Office deemed adequate - to remedy the violation and mitigate its possible negative effects on the interested parties (see note of 31 July 2020).

From the assessment carried out on the basis of the elements acquired as well as the subsequent evaluations, it appears that the candidates have proceeded to register for the aforementioned competition organized by the Region, through the portal in question, and that, in the days preceding the pre-selection tests, the same sent to the Company, provider of the organization and management service of the pre-selection phase, responsible for the treatment, the data necessary for carrying out these tests (name, surname, date of birth and tax code of each participant in the procedure). Subsequently, the Company proceeded to "upload" the data relating to the tests carried out on the server that would host the web application for each candidate to consult their data. In this circumstance, the security incident occurred which gave rise to the dissemination of numerous personal data (referring to approximately 3,600 participants in the pre-selection phase on 21, 22 and 23 July 2020).

On this point, it is noted that the data controller is required to "implement adequate and effective measures [and ...] demonstrate the compliance of the processing activities with the [...] Regulation, including the effectiveness of the measures" adopted (recital 74 of Regulation) and, in this context, for the purpose of preparing the technical and organizational measures that meet the requirements established by the Regulation, a person in charge of carrying out certain processing activities may also be used, to whom he / she gives specific instructions, also in terms of security (see recital 81 of the Regulation).

According to the Regulation, the data must be "processed in such a way as to guarantee adequate security of personal data, including protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage. "(Article 5, par. 1, letter f), of the Regulations).

In any case, the owner remains responsible for implementing the appropriate technical and organizational measures to ensure and be able to demonstrate that the processing is carried out in accordance with the Regulations. In fact, the data controller falls within the decisions regarding the purposes and methods of processing the personal data of the interested parties as well

as a "general responsibility" in relation to the treatments put in place (see art. 5, par. 2 which formalizes the 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; prov. 17 September 2020, n. 160 doc. web n. 9461168 and, lastly, prov. 10 June 2021, n. 235, doc. web n. 9685922).

To this end, in order for the data controller to be in a position to comply with its data protection obligations and to be able to prove it, the agreement governing the relationship with the data controller must have a sufficient level of detail in this regard. to these measures (articles 5, paragraph 2, and 24 of the Regulation; see, on this point, with express reference to the relationship between articles 5, paragraph 2, 24 and 32 of the Regulation Guidelines 7/2020 on the concepts of controller and processor in the GDPR, adopted by the European Data Protection Committee on 7 July 2021, in particular, par. 2.1.4, points 8, 19, 41 and 126).

In the present case, it emerged that the Region, with the contract for the assignment of the service, has regulated, pursuant to art. 28 of the Regulation, the relationship with the Company, providing that the Company undertakes "not to implement, for any reason, data processing other than those authorized by the Data Controller" and the subject of the contract (see art. 16 of the aforementioned service contract).

In particular, albeit in the technical offer which is an integral part of the aforementioned contract, the Company, responsible for the processing, also undertook to guarantee "immediately after the conclusion of the tests, online access to the documents, the personal data sheet, of the matching code and the corrector to the Candidate who, with username and password, can view his / her work "(Annex 3 to the note of the Tuscany Region of 20 November 2020, p. 31), it is ascertained that, in carrying out the necessary activities the preparation of the web application for consultation by each candidate of their data, the Company had not, however, adopted any suitable measure to ensure that the personal data of each interested party were made available exclusively to the same or to authorized subjects.

In particular, the failure to adopt computer authentication procedures - on the occasion of the aforementioned data upload operation, on 29 July 2020, from 14:49 to 15:49 - made it possible for anyone who connected to the web address https://scanshareservice.com/regione-toscana/, however erroneously made available to a candidate, to freely access the personal data of the approximately 3,600 interested parties participating in the procedure (i.e., name, surname, date of birth, tax code, day test and convocation session, number of questionnaire extracted for the session in which each candidate

participated, detailed results of the individual questionnaires and overall score).

This has given rise to the dissemination of personal data, processed in the context of the aforementioned insolvency procedure launched by the Region and for which the same must be held responsible according to the Regulations (Articles 5, par. 2, and 24 of the Regulations). The defensive arguments of the same, even if taken into due consideration for the purposes of this provision, are not in fact sufficient to completely exclude the responsibility of the data controller with regard to the obligations deriving from the regulations on the protection of personal data.

Given the above, the absence of technical and organizational measures adequate to the risks associated with the specific data upload operation - even though it is mainly attributable to the failure to prepare specific access control measures on the server in question by the Company, the data processor - has created the conditions for the occurrence of the security breach that led to the online disclosure of the candidates' personal data, in violation of Articles 5, par. 1, lett. a), and 6, par. 1, lett. c) and e), of the Regulations and art. 2-ter of the Code, of which the Region, the data controller, must in any case be held responsible pursuant to art. 5, par. 2 and 24 of the Regulation.

4. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the data controller during the investigation the truthfulness of which one may be called to respond pursuant to art. 168 of the Code , although worthy of consideration, do not allow to overcome the findings notified by the Office with the act of initiation of the procedure and are insufficient to allow the dismissal of this proceeding, since none of the cases provided for by the 'art. 11 of the Guarantor Regulation n. 1/2019.

Therefore, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by the Tuscany Region is noted, in relation to the dissemination of personal data relating to numerous candidates of the aforementioned competition procedure and numerous information relating to the preselective tests. carried out by the same, also including the outcome and the vote obtained by each, in violation of art. 5 and 6 of the Regulations and art. 2-ter of the Code (in the text prior to the amendments referred to in Legislative Decree No. 139 of 8 October 2021).

The violation of the aforementioned provisions makes the administrative sanction provided for by art. 83, par. 5, of the Regulation, pursuant to art. 58, par. 2, lett. i), and 83, par. 3, of the same Regulation and art. 166, paragraph 2, of the Code.

In this context, considering, in any case, that the conduct has exhausted its effects, the conditions for the adoption of further 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.

In relation to the aforementioned elements, the high number (over three thousand participants in the competition) of interested parties whose data were disclosed was considered.

On the other hand, it was considered that the violation of the personal data in question - which however lasted for a short period of time (about an hour) - was mainly attributable to the failure to prepare specific security measures by the data controller and that the data controller, after becoming aware of the same, has taken adequate measures to remedy it and mitigate the possible negative effects on the interested parties. The Region also lent its extensive cooperation during the investigation.

There are no previous relevant violations committed by the data controller or previous provisions pursuant to art. 58 of the Regulation.

On the basis of the aforementioned elements, evaluated as a whole, it is believed to determine the amount of the pecuniary sanction, in the amount of € 10,000 (ten thousand) for the violation of Articles 5 and 6 of the Regulations and art. 2-ter of the Code (in the text prior to the amendments referred to in Legislative Decree no. 139 of 8 October 2021), as a withholding administrative fine, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

Taking into account the numerous interested parties involved in the violation of the aforementioned data, it also believes that the ancillary sanction of the 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

pursuant to art. 57, par. 1, lett. f), of the Regulations, declares unlawful the conduct of the Tuscany Region, described in the terms set out in the motivation, consisting in the violation of articles 5 and 6 of the Regulations and art. 2-ter, of the Code (in the text prior to the amendments referred to in Legislative Decree No. 139 of 8 October 2021), within the terms set out in the motivation;

ORDER

to the Tuscany Region, in the person of the pro-tempore legal representative, with registered office in Florence (FI), Piazza Duomo 10, C.F. 01386030488, pursuant to articles 58, par. 2, lett. i), and 83, par. 5, of the Regulations and art. 166, paragraph 2, of the Code, to pay the sum of € 10,000 (ten thousand) as a pecuniary administrative sanction for the violations indicated in the motivation;

INJUNCES

the Tuscany Region to pay the sum of € 10,000 (ten thousand) according to the methods indicated in the annex, within 30 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. In this regard, it is recalled that the offender has the right to settle the dispute by paying - again according to the methods indicated in the annex - of an amount equal to half of the sanction imposed, within 30 days from the date of notification of this provision, pursuant to art. 166, paragraph 8, of the Code (see also Article 10, paragraph 3, of Legislative Decree no. 150 of 1/9/2011);

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, 152 of the Code and 10 of Legislative Decree no. 150/2011, 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, February 10, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei