[doc. web n. 9754332]

Order injunction against Scanshare S.r.l. - February 10, 2022

Record of measures

n. 44 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.

2. The preliminary activity.

With the notes of 10 September 2020, the Company, in response to the request for information formulated by the Office, stated, in particular, that:

“Following the request of a candidate […] our IT manager communicated the link that would host the portal and to which access to verify his / her work; accidentally, this link coincided with the name of the folder in which the data upload was in progress from 14:49 to 15:49 of 27/07/2020. The candidate then shared the link in a whatsapp group. It is assumed that the participants in the group have had access to the uploaded data. It is specified that the upload lasted an hour, but only at the end of the upload did the folder contain the complete data, which were accessible, to those who knew the link, only for a few minutes. The sharing of information took place through "word of mouth" between the candidates ";

"Each candidate can access their data on the computer application for access to the tests, which has been moved to another URL than the one that is the subject of the violation. To access their data, the user must enter: registration number of the applications for participation in the competition, the email address indicated in the application for participation in the competition and tax code. The candidate has access only and exclusively to the data relating to his / her competition test: Surname, name, date of birth, tax code, protocol number of the application form, score and optical reading of the pre-selection test answer form. Neither the application database, nor the data subject to the violation, contain documentation produced at the time of submitting the application to participate in the competition, other than that listed above ";

"The data upload process took place with an ftps transmission to the hosting space that would host the web application. At the time of the violation, there were no other access restrictions as part of the application still being uploaded "and that" [...] the file that could be downloaded in full, in those few minutes, was not easy to read and totally in "clear" and contained some data, previously published on the Tuscany Region website, relating to the call of candidates; in addition there were the date of birth, the tax code, the protocol number of the application, the optical reading string and the score obtained by each candidate ";

in other respects, the company declared that it had initiated some analyzes, also with the support of Hostinger International Ltd, based in Cyprus (hereinafter "Hostinger"), which carries out hosting services, in order to determine the number, even approximate , of subjects who have made unauthorized access to personal data subject to violation. As a result of the aforementioned checks, it emerged that "only for a few minutes the complete data were accessible to those who knew the link, it is presumed that the file circulated among the candidates not because it was downloaded directly from the link but by word of mouth".

With a note dated 4 December 2020, the Office, on the basis of the elements acquired, the verifications carried out and the facts that emerged as a result of the investigation, 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, concerning the alleged violations of articles 28, par. 2, and 32 of the Regulations, inviting you 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 Law 24 November 1981, no. 689).

The Company sent its defense briefs with a note dated January 2, 2021, representing, among other things, that:

"The relationship between Scanshare Srl and the Region of Tuscany is governed by a framework agreement having as its object the management and organization of insolvency procedures launched by the Region. In compliance with this framework agreement, Scanshare performed these services relating to the Public Competition for 84 Administrative Assistants. The pre-selection tests were held at Arezzo Fiere on 21 - 22 - 23 July 2020. There were 13,882 candidates registered, at the end of the tests 3548 candidates were present during the test. Among the services provided for the Tuscany Region, for the purposes of transparency and confidentiality of the procedure, Scanshare made available a portal through which candidates, with personal credentials, could each access their own test by viewing the image of the Answers form. , the personal data sheet, the questionnaire, the corrector and the score obtained ";

"In the days following the performance of the tests, Scanshare prepared the portal and the documentation to be published to allow candidates to view their test, each candidate could have access to their consultation page using the following credentials: application protocol number and code tax. Before the official publication of the portal and following a request from a candidate, our IT manager erroneously communicated the link that would have hosted the portal to be accessed for verifying his / her work; accidentally, this link coincided with the name of the folder in which the data upload was in progress made from 14:49 to 15:49 of 27/07/2020 ";

"The IT manager, who replied to the candidate's email, is a different person from the IT staff who took care of the upload, fortuitously, they both chose the same name for the portal link and the name of the upload folder . The candidate then shared the link in a whatsapp group; it is assumed that the participants in the group have had access to the uploaded data. It is specified that the upload lasted an hour, but only at the end of the upload did the folder contain the complete data, which were accessible, to those who knew the link, only for a few minutes ";

“The sharing of information took place through“ word of mouth ”between the candidates. The data upload process took place with an ftps transmission to the hosting space that would host the web application. The data that could be consulted at the end of the upload, for a very few minutes, were as follows: Surname, name, date of birth, tax code, protocol number of the application, score and optical reading of the pre-selection test answer form. Neither the application database, nor the data subject to the violation, contain documentation produced at the time of submitting the application to participate in the competition, other than that listed above [...]. Furthermore, it should be noted that the downloadable file in its entirety, in those few minutes, was not easy to read and totally in "Clear" and contained some data, previously published on the Tuscany Region website, relating to the call of candidates ";

the Company has adopted some measures to mitigate the effects of the violation for the parties concerned;

“With reference to the Hostinger company, it is confirmed that it cannot be configured as a sub-manager. In the days following the unauthorized access to the data, the Hostinger company was contacted by us, exclusively for exploratory purposes, to check if it could access the logs in order to communicate the number of accesses to the folder to the Tuscany Region and to this esteemed Authority. The Hostinger company, however, as we have already stated, was unable to communicate the logs to us and did not have access in any way to the data contained in the space made available to us. For these reasons, having contacted Hostinger cannot be considered as proof that this company can be configured as a sub responsible ".

Furthermore, the Company, during the hearing, pursuant to art. 166, paragraph 6, of the Code, represented that (see minutes of 20 April 2021):

"The violation of personal data was caused by a non-malicious computer accident";

“The Company points out that the Regional Administrative Court for Tuscany, section 1, with sentence of 29 April 2020, no. 518, it ruled establishing that, in the context of the exercise of access to the documents, the applications, the documents produced by the candidates and the other documents of the competition procedures constitute documents with respect to which the need for confidentiality to protect of third parties ";

"Therefore, this orientation of administrative jurisprudence, even if in a different context, can be taken into consideration in the evaluation of the conduct that is the subject of the procedure as the personal data subject to violation - which have been consulted, for a few minutes, by the candidates in the competition - they could have been the subject of requests for access to the documents by the candidates themselves ";

"The Company believes that, although during the investigation it emerged that Hostinger was requested to provide a copy of the access logs to the IT systems involved in the violation of personal data, the hosting service provider is not a data processor in how much does not have access to personal data hosted on their systems ".

3. Outcome of the preliminary investigation.

3.1. The regulatory framework.

The personal data protection discipline provides that, although the data controller, who determines the purposes and methods of data processing, falls under a "general responsibility" for the treatments put in place (see art. 5, par. 2 , the so-called principle of "accountability", and 24 of the Regulation), even when these are carried out by other subjects "on its behalf" (cons. 81, articles 4, point 8), and 28 of the Regulation), the Regulation, in each case, has established specific obligations and regulated the other forms of cooperation to which the data controller is required and the scope of the related responsibilities (see articles 30, 32, 33, par. 2, 82 and 83 of the Regulation) .

The data controller, in fact, is entitled to process the data of the interested parties "only on the documented instruction of the owner" (Article 28, par. 3, letter a), of the Regulation) and the relationship between the owner and manager is governed by a contract or other legal act, stipulated in writing which, in addition to mutually binding the two figures, allows the owner to give instructions to the person in charge also from the point of view of data security and provides, in detail, which subject is

governed, the duration, nature and purposes of the processing, the type of personal data and the categories of data subjects, the obligations and rights of the owner and manager.

The manager cannot, in turn, resort to another manager "without the prior written, specific or general authorization of the data controller" and, if so, "the same obligations are imposed on this other data controller [...] of data protection, contained in the contract or other legal act between the data controller and the data processor "(Article 28, par. 2 and 4, of the Regulation).

Furthermore, art. 32 of the Regulation provides that, not only the owner, but also the manager, within the scope of his / her competences and the tasks delegated by the owner, "taking into account the state of the art and the costs of implementation, as well as the nature, the context and purposes of the processing, as well as the risk of varying probability and severity for the rights and freedoms of natural persons "must implement" adequate technical and organizational measures to ensure a level of security appropriate to the risk "and that" in assessing the adequate level of security, special account is taken of the risks presented by the processing which derive in particular […] from the unauthorized disclosure [… of] personal data transmitted, stored or otherwise processed ".

3.2. The security of the processing.

Preliminarily, it is noted that the Company, after becoming aware of the violation of personal data, has provided assistance to the owner in ensuring compliance with the obligations regarding the security of processing, also with regard to the measures taken to remedy and mitigate the negative effects of the violation on the interested parties (articles 28, par. 3, letter f), and 32, of the Regulation).

From the assessment carried out on the basis of the elements acquired, as well as the subsequent assessments of the Office, 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 has sent to the Company, provider of the organization and management service of the pre-selection phase, responsible for the treatment, the data necessary to carry 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).

It is ascertained that, in carrying out the activities necessary for the preparation of the web application for the 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 interested party 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 in question (i.e., name, surname, date of birth, tax code , day of the test and call session, number of questionnaire extracted for the session in which each candidate participated, detailed results of the individual questionnaires and overall score).

In the present case, the violation of personal data occurred for reasons attributable mainly to the Company that processed the data in its capacity as data processor. In particular, given the absence of specific access control measures to limit data processing to interested parties or authorized subjects only, it is believed that the technical and organizational measures adopted by the Company have not been adequate to the risk and that this has resulted in a violation of art. 32 of the Regulation.

Nor can what is represented by the Company be considered relevant in relation to the right of access to administrative documents, traditionally recognized by administrative jurisprudence for candidates in bankruptcy proceedings, a circumstance that does not occur in the present case, as a security incident has instead occurred which involved a online dissemination of personal data.

3.3. The use of the hosting service provider.

Although the Company, in providing the identification details of the hosting service provider it uses (Hostinger), has represented that the same "does not have access to the database in any way, does not intervene in any way in the processing of personal data "And that, with reference to the processing of personal data in question," no sub-manager has been appointed and / or used ", however, during the investigation a report was produced by the Region, sent by the Company, from which emerges that it represented that it had asked Hostinger for the "logs of the IP addresses that had access to the data".

In this regard, it should be noted that given the definition of "processing of personal data" (Article 4, point 2) of the Regulation) and as also reported in the so-called "Privacy Policy" (spec. Par. "6. Information pertaining to visitors and users of our user's

websites or services") published on the Hostinger website (URL: https://www.hostinger.it/privacy), the provider of the hosting service in question - be it hosting of websites on shared servers, or hosting of virtual or physical servers - processes personal information relating to visitors or users of a website hosted on its technological infrastructure. Firstly, Hostinger collects, records and stores some personal data whose transmission is implicit in the use of telematic communication protocols, such as the IP address of the device used by the user, the date and time of the connection and the IP address of the server hosting the website visited by the user. Furthermore, while not directly accessing personal data processed within a website, Hostinger, as a hosting service provider, retains such data on its technological infrastructure, ensuring certain levels of service in terms of system availability and providing provision of its customers with a series of tools to manage and monitor the service (see, with regard to the failure to regulate the relationship with the hosting service provider, provision 11 February 2021, no. 49, web doc. no. 9562852, spec. par. 3.2).

Based on the above elements, it must therefore be considered that, contrary to what the Company claims, the operations described above still give rise to the processing of personal data pursuant to art. 4, point 2), of the Regulation, by Hostinger (see 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, point 40, in the part where the example relating to "Hosting services" is reported).

Furthermore, it is noted that during the investigation the Tuscany Region highlighted that "it has not received any communications or requests for authorization from the Company Scanshare S.r.l. regarding the involvement of third parties and their appointment as sub-processors for the processing of data "(see, with regard to the lack of authorization of the holder to have recourse to another data controller, provision 10 June 2021, no. 236, web doc. no. 9685947, spec. par. 3.1).

For these reasons - also considering that art. 16 of the "contract for the award of the service" Organization and management of the preselection of the competition tests ", which governs, pursuant to art. 28 of the Regulation, the processing of personal data under examination by the Company, in its paragraph 3 provides that "the contractor undertakes not to implement treatment other than those authorized by the owner" - it is believed that the appeal by the Company to the services offered by Hostinger, without prior written authorization from the Tuscany Region, has occurred in violation of art. 28, par. 2, 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 Company, on behalf of the Tuscany Region, is noted, as entrusted with the management service of certain phases of the aforementioned procedure, as it occurred in absence of adequate technical and organizational measures aimed at guaranteeing the confidentiality and integrity of personal data processed in violation of art. 32 of the Regulations and by resorting to a company for the hosting service without the prior written authorization of the data controller, in violation of art. 28, par. 2, of the Regulation.

The violation of the aforementioned provisions makes the administrative sanction provided for by art. 83, par. 4, 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, the violation of the aforementioned provisions is subject to the application of the same administrative fine provided for by art. 83, par. 4, 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 personal data lasted for a short period of time (about an hour) and that the Company provided its extensive cooperation during the investigation.

For the purposes of measuring the overall sanction, the Company's turnover was also considered as resulting from the last financial statements, as well as the fact that the Company itself was involved in a previous proceeding, later defined with provision no. 161 of 17 September 2020 (web doc. 9461321), during which it was ascertained that the same, in the management of certain phases of an insolvency procedure launched by another public client, had become responsible for a related security incident to the data contained in the applications for participation in the competition. For these reasons, it is believed that the previous violations committed by the Company must be considered specific precedents "relating to the same object" (Article 83, paragraph 2, letter i), of the Regulation) in relation to the failure to adopt adequate security measures (Article 32 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 28, par. 2, and 32 of the Regulations, as a pecuniary administrative sanction, 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 company Scanshare S.r.l., described in the terms set out in the motivation, consisting in the violation of articles. 28, par. 2, and 32 of the Regulations, within the terms set out in the motivation;

ORDER

to the company Scanshare S.r.l. in the person of the pro-tempore legal representative, with registered office in Rende (CS),

C.da Cutura 7, P.I. 03118780786, pursuant to art. 58, par. 2, lett. i), and 83, par. 5, of the Regulation and 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

to the company Scanshare S.r.l. 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