SEE ALSO Newsletter of 26 October 2020

[doc. web no. 9469345]

Provision on data breach - 1st October 2020

Register of measures

no. 174 of 1 October 2020

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 Dr. Claudio Filippi, deputy secretary general;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as well as on the free circulation of such data and repealing Directive 95/46 /CE, "General Data Protection Regulation" (hereinafter "Regulation");

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national legal system to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons with regard to the processing of personal data, as well as to the free movement of such data and which repeals Directive 95/46/EC (hereinafter the "Code");

CONSIDERING the Regulation n. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved with resolution no. 98 of 4/4/2019, published in the Official Gazette no. 106 of 8/5/2019 and in www.gpdp.it, doc. web no. 9107633 (hereinafter "Regulation of the Guarantor n. 1/2019");

HAVING REGARD to the documentation in the deeds;

GIVEN the observations made by the deputy secretary general pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the Guarantor's office for the protection of personal data, doc. web no. 1098801;

Speaker the lawyer Guido Scorza;

WHEREAS

1. The personal data breach.

The Campus Bio-medico University of Rome (hereinafter Campus Bio-medico) has notified the Guarantor of a personal data

breach pursuant to art. 33 of the Regulation relating to the "system through which the online consultation service of reports is provided to the public", following which some users were able to view "data relating to health, in particular radiological images associated with identification data and clinical reports" of 74 other users (communication of the XX, prot. n. XX).

According to what was notified, "the personal data subject to the violation have been viewed by a limited number of specific subjects (at present, no more than 39 users), and that these subjects, as patients/users on the same level as the interested parties, are, presumably, in the same condition as the latter and therefore - probably - without any interest in using/disseminating such information, especially for malicious ends". In the aforementioned communication it was also specified that "during the integration between the Carestream system (CSAP-MyVue) and the patient portal "MyHospital", due to a human error in the configuration of this integration some users of the aforementioned portal (only those who accessed via mobile device) were able to view personal data relating to other users" and that, "after receiving the report of the incident, steps were taken immediately to interrupt the image publication service and of radiology reports online. At the same time, a notification was made to the system supplier (Carestream)" who "identified the causes of the problem and proceeded to make the following corrective actions: Reset of the integration parameter, in order to prevent further actions; Checks carried out in both test and production environments, which confirmed that unauthorized access to user data can no longer occur; The integration knowledge-base has been updated and contains the recommendation to use the "User Token" for a more robust workflow".

With the subsequent integration of the aforementioned notification, the Campus Bio-medico represented that "in all 74 cases found, no download of the data appears to have been carried out" and that "many of the illicit accesses occurred in a period of time ranging from 2016 to 2018" (note of the XX).

With a note dated XX, Campus Bio-medico also represented that "the sequence that leads to the problem was the following: the user accessed the My-Hospital service, using a smartphone browser, using a username and password. Then, by entering the secret code, he accessed the section relating to the download of documents where he could view the list of any reports produced in the last 45 days. If the report was linked to images, the user selected the "view images" button and correctly displayed the images relating to the selected clinical episode. If the user, having reached this point, instead of exiting, had selected the "back" button, he would have seen on the MyVue portal - as expected - his name from which it would have been possible to access his images again. However, if at this point the user had selected the "back" button again, he would have

seen the alphabetically sorted list of all users on the MyVue portal, from which he could have selected a name other than his own and then displayed the list of examinations and related images, which has occurred in 39 cases over the years. As previously mentioned, the same procedure carried out from the desktop browser does not highlight any anomaly".

Subsequently, with the communication of the XX the Campus Bio-medico then specified that 25 of the aforementioned accesses were made in the "period between 25 May 2018 and 4 August 2019".

2. The preliminary investigation.

The Office, with deed n. XX of the XX, notified the Campus Bio-medico, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in article 58, paragraph 2, of the Regulation, inviting the aforesaid holder to produce defense writings or documents to the Guarantor 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, of law n. 689 of 11/24/1981).

In particular, the Office, in the aforesaid deed, represented that, even if the conduct object of the preliminary investigation by the Office began before the date of full application of the Regulation, in order to determine the applicable rule in terms of time, it must be recalled the principle of legality pursuant to art. 1, paragraph 2, of the law n. 689 of 11/24/1981 which provides that «The laws that provide for administrative sanctions are applied only in the cases and within the times considered in them». The application of this principle determines the consequence of taking into consideration the provisions in force at the time of the violation committed. In the present case, this moment - considering the permanent nature of the contested conduct - must be identified as the moment of cessation of the unlawful conduct, which from the preliminary investigation documents appears to have lasted at least until 4/8/2019, i.e. after the 25/5/2018, date on which the Regulation became fully applicable.

In the aforesaid deed, the Office found that, on the basis of the elements acquired and the facts that emerged following the preliminary investigation, the Campus Bio-medico, by allowing access to users of the MyVue mobile app to health data (images radiological data, personal data and reports) of 74 interested parties, made a communication of particular categories of data of the interested parties to third parties in the absence of a suitable legal prerequisite and, therefore, in violation of the basic principles of the treatment referred to in articles 5 and 9 of the Regulation. In particular, it was represented that the aforementioned processing of personal data was carried out in a manner that did not comply with the principles of "lawfulness, correctness and transparency", as well as "integrity and confidentiality" of the processing, in violation of art. 5, par. 1, lit. a) and f) of the Regulation and in the absence of a suitable regulatory prerequisite, in violation of articles 75 of the Code and 9 of the

Regulation.

With a note of the XX, the Campus Bio-medico sent its defense briefs, in which further elements were represented and in particular that:

- "Due to the aforementioned violation, some users, during a period of time ranging from November 25, 2016 to August 2019, were able to view health-related data, specifically radiological images associated with identification data and clinical reports, of other 74 users";
- "Moreover, regarding the bug in question, it should be emphasized that this would not appear to correspond to any pattern known in the literature as vulnerable, but rather to a logic bug introduced by the supplier during the integration of its product with the MyHospital system". "Notwithstanding the foregoing, consider that if the supplier had complied with the guidelines for the development of secure software or had carried out VAPT activities on such systems, these, in all likelihood, could have prevented - in the first case - or, in any case, limit over time - in the second case - the data breach";
- "the operating anomaly in question occurred only in the mobile version (and not in the one used on a PC browser) of the MyVue application of the former Carestream Health Italia S.r.l. supplier, and how the other services displayed on the MyHospital portal are not involved ";
- "as soon as it becomes aware of the event, the Data Controller has promptly: (i) suspended the service; (ii) reported the event to the system provider to enable him to identify the problem and remedy it permanently; (iii) effectively implemented all the appropriate technical and organizational measures aimed at verifying whether a violation of personal data could be considered configured; (iv) informed the supervisory authority";
- "As known, the censored behaviors can be linked to an event generated by a human configuration error in the integration between the Carestream system (CSAP-MyVue) and the patient portal "MyHospital", as the operator appointed by the supplier of the service set - quite accidentally - the boolean value "true" instead of "false";
- "according to what emerges from the evidence relating to the survey on access logs carried out by the technical staff of the supplier company that manages the Carestream Health Italia S.r.l. (today Philips S.p.A. following the sale of the company branch), the aforementioned data breach resulted in the loss of confidentiality of a rather limited amount of personal data (125), moreover referring to only 74 other users (interested) on a total of 30,000 users who made use of the online reporting service in question in the reference period. In addition, the scope of knowledge of such information was limited to only 39 other

users (of the service);

- "the Owner has not received any complaints or requests for compensation for damages related to the violations in question, where it is considered that part of the accesses date back over time (i.e. to 2016)".

3. Outcome of the preliminary investigation.

Having taken note of what is represented by the Campus Bio-medico in the documentation in the deeds and in the defense briefs, it is noted that:

1. the Regulation, in establishing a general ban on the processing of particular categories of personal data, provides for a derogation in the event that the processing is necessary for the purposes of diagnosis, assistance and health therapy (Article 9, paragraph 2, lett. h) and par. 3 of the Regulation) and is carried out on the basis of the law of the Union or of the Member States (see in this regard art. 12, legislative decree n. 179/2012, Prime Ministerial Decree n. 178/2015). The processing of personal data in question can be traced back to the cases indicated in the art. 9, par. 2, lit. h) of the Regulation;

2. the IT error described above determined, in a period of time ranging from 25 November 2016 to August 2019, the possibility that users of the online medical reports consultation service could view data relating to health, specifically the images radiological data associated with identification data and clinical reports, of 74 other users and which is documented in documents that the aforementioned data were viewed by 39 users.

4. Conclusions.

In the light of the assessments referred to above, taking into account the statements made by the data controller during the preliminary investigation and considering that, unless the fact constitutes a more serious crime, anyone who, in a proceeding before the Guarantor, falsely declares or certifies or circumstances or produces false deeds or documents, it is liable pursuant to art. 168 of the Code "False declarations to the Guarantor and interruption of the execution of the duties or the exercise of the powers of the Guarantor" the elements provided by the data controller in the defense briefs do not allow to overcome the findings notified by the Office with the deed of initiation of the proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the Campus Bio-medico University of Rome in the terms set out in the justification, for violation of articles 5, par. 2, lit. a) and f), and 9 of the Regulation and of the art. 75 of the Code.

In this context, considering, in any case, that the conduct has exhausted its effects, given that the Campus Bio-medico has declared that the IT error that caused, in a period of time ranging from 25 November 2016 to August of 2019, the possibility that users of the online report consultation service could view health-related data, specifically the radiological images associated with identification data and clinical reports, of 74 other users, has been corrected, the conditions for the adoption of the 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 accessory sanctions (articles 58, paragraph 2, letter i and 83 of the Regulation; article 166, paragraph 7, of the Code).

The violation of the articles 5, par. 2, lit. a) and f), and 9 of the Regulation and of the art. 75 of the Code, caused by the conduct carried out by the Campus Bio-medico University of Rome, is subject to the application of the administrative fine pursuant to art. 83, par.5, lett. a) of the Regulation.

Consider that the Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, has the power to "impose a pecuniary administrative sanction pursuant to article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, according to the circumstances of each single case" and, in this context, "the Board [of the Guarantor] adopts the injunction order, with which it also orders the application of the ancillary administrative sanction of its publication, in whole or in part, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code" (art. 16, paragraph 1, of the Guarantor's Regulation no. 1/2019).

The aforementioned pecuniary administrative sanction imposed, depending on the circumstances of each individual case, must be determined in the amount taking into account the principles of effectiveness, proportionality and dissuasiveness, indicated in art. 83, par. 1, of the Regulation, in the light of the elements provided for in art. 85, par. 2, of the Regulation in relation to which it is observed that:

- the Authority became aware of the event following the personal data breach notification made by the same controller and no complaints or reports were received to the Guarantor on the incident (Article 83, paragraph 2, letter a) and h) of the Regulation);

- the data processing carried out by Campus Bio-medico, through the online reporting service, concerns data suitable for detecting information on the health of many interested parties. The event resulted in the accessibility, by the users of the MyVue mobile app, to the health data (radiological images, personal data and reports) of 74 interested parties, in a period of

time ranging from 25 November 2016 to August 2016. 2019 (Article 4, paragraph 1, no. 15 of the Regulation and Article 83, paragraph 2, letter a) and g) of the Regulation);

- the absence of voluntary elements on the part of Campus Bio-medico in causing the event (art. 83, paragraph 2, letter b) of the Regulation);

- the immediate taking charge of the problem followed by the identification of corrective and resolution solutions (Article 5, paragraph 2 and Article 83, paragraph 2, letters c) and d) of the Regulation);

- the holder has immediately demonstrated a high degree of cooperation (Article 83, paragraph 2, letters c), d) and f) of the Regulation).

Based on the aforementioned elements, evaluated as a whole, also taking into account the phase of first application of the sanctioning provisions pursuant to art. 22, paragraph 13, of Legislative Decree lgs. 10/08/2018, no. 101, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 4, lit. a) and par. 5, letter. b) of the Regulation, to the extent of 20,000 (twenty thousand) euros for the violation of articles 5, par. 1, lit. a) and f) and 9 of the Regulation and 75 of the Code as a pecuniary administrative sanction withheld, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary sanction of publication on the Guarantor's website of this provision should be applied, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Regulation of the Guarantor n. 1/2019, also in consideration of the potential number of interested parties and the type of personal data subject to unlawful processing.

Finally, it should be noted that the conditions pursuant to art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

ALL THIS CONSIDERING THE GUARANTOR

declares the illegality of the processing of personal data carried out by the Campus Bio-medico University of Rome, for the violation of the articles 5, par. 2, lit. a) and f), and 9 of the Regulation and of the art. 75 of the Code in the terms referred to in the justification.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the Campus Bio-medico University of Rome with registered office in Rome, in via Álvaro del Portillo 200, P. Iva 04802051005 / C. F. 97087620585, in

the person of its pro-tempore legal representative, to pay the sum of 20,000 euros (twenty thousand) as a pecuniary administrative sanction for the violations indicated in this provision, according to the methods indicated in the attachment, within 30 days of the notification in the motivation; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the fine imposed.

ENJOYS

to the aforementioned Campus Bio-medico to pay the sum of 20,000 (twenty thousand) euros, according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the law n. 689/1981. In this regard, it is recalled that the offender retains the right to settle the dispute by paying - always according to the methods indicated in the annex - an amount equal to half of the fine imposed, within 30 days from the date of notification of this provision, pursuant to art. 166, paragraph 8, of the Code (see also art. 10, paragraph 3, of Legislative Decree no. 150 of 09/01/2011);

HAS

pursuant to art. 166, paragraph 7, of the Code, the entire publication of this provision on the website of the Guarantor and believes that the conditions set forth in art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

Pursuant to art. 78 of the Regulation, of the articles 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision it is possible to lodge an 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 appellant resides abroad.

Rome, 1st October 2020

PRESIDENT

Station

THE SPEAKER

Zest

THE DEPUTY SECRETARY GENERAL

Philippi