[doc. web n. 9586906]

Injunction order against the Italian Diagnostic Center of Milan - March 25, 2021

Record of measures

n. 118 of 25 March 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stazione, president, Professor Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, members, and the Cons. Fabio Mattei, general secretary;

GIVEN the Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46 / EC, "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;

GIVEN 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;

Rapporteur, the lawyer Guido Scorza;

WHEREAS

1. The violation of personal data and the investigation activity

The Italian Diagnostic Center - CDI (hereinafter the Center) has notified this Authority three violations of personal data pursuant to art. 33 of the Regulation concerning:

1. the successful delivery to a patient of a report relating to another patient, due to the "homonymy of the surname" and the "assonance of the name"; the report was subsequently returned to the Customer service staff of the Center (event of 22 October 2018, communication of violation of 24 October 2018). Following a request for information from the Office (note dated 29.1.2019, prot.n.3060), the Center declared that the erroneous delivery of the report depended on the incorrect application of the patient identification procedure, "Reading by means of a scanner gun", and to have made the Customer service staff aware of the importance of a correct comparison between the identification label applied on the envelope and the documents contained therein (note of 28 February 2019);

2. the display, by the patient within the online reporting system of the aforementioned Center, of diagnostic images relating to another patient, accompanied by the personal data of the latter (event of 19 December 2018, communication of violation of 21 December 2018);

3. the successful delivery to a patient of a report relating to another patient due to the "assonance of the surname"; the report was subsequently returned to the Center (event of 13 February 2019, communication of violation of 15 February 2019).

With reference to the processing of personal data carried out by the aforementioned Center, the Office also received a complaint from an interested party who, after having contacted the Center for some health services, had found, in his Electronic Health Record (FSE), the reports of other users of the Center, in place of their own. In this regard, in response to a request for information from the Office (note of 23 January 2019, prot. No. 2422), the aforementioned Center stated that the "incorrect attribution of the reports of another patient to the registry" of the complainant , during the process of publication of the report in the FSE, "originated in the acceptance process of the other patient, performed in the SSN regime, and was caused by a technical run-time error in the CDI acceptance system that created a misalignment between the master data present in the CDI system and that acquired by the Lombardy Region system and used by the CDI in the process of subsequent publication of the report on the ESF "(note of 22 February 2019). The aforementioned Center also represented that it had introduced "a blocking control during the process of publishing the reports on the FSE of the Lombardy Region" and that it had started the implementation of "an IT block where the verification of alignment of the patient's unique identification data fails ".

In this regard, the Office, with the notes of April 4, 2019 (prot. No. 11654) and April 16, 2019 (prot. No. 13072), notified the Italian Diagnostic Center, 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 holder to produce defensive 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, by law n. 689 of 24/11/1981).

In particular, the Office found that, on the basis of the elements acquired and the facts that emerged as a result of the investigation, the Center in the cases described above, relating to the delivery of reports - even digitally - and through the attribution of a patient report to another patient's Electronic Health Record, communicated data relating to the health of four interested parties to other subjects in the absence of a suitable legal basis and, therefore, in violation of the basic principles of the treatment referred to in articles 5 and 9 of the Regulation.

With a note dated May 15, 2019, the Center sent its defense briefs, in which additional elements were represented and in particular:

- with reference to the communication of violation of 24 October 2018, that "the person in charge probably proceeded to deliver the envelope with the report only on the basis of reading the identification data shown on the envelope itself, without carrying out the reading operation automated by means of a scanner gun, which did not allow to be able to repair the involuntary oversight of the same person in charge who did not notice the diversity of the names reported, next to the same surname, on the sealed envelope containing the report; both the person delegated to collect the envelope with the report and the reporting patient did not immediately realize that the envelope with the report was referring to a different patient with the same surname but with a different name, and obviously, the envelope being closed and reporting the data of a patient with a different name externally, the reporting person also opened it by mistake and thus became aware, albeit for a brief moment, of the report in the same content, from which they could also be deduced personal data relating to the health of another patient ". Following the incident, the Center proceeded to "send a communication to raise the awareness of the Customer Service staff about the importance of strictly following the verification procedure which involves the use of the scanner gun supplied for correct identification. of the report "; to "a verbal warning by the HR manager to personnel who did not comply with the procedures and instructions specifically given"; the "provision of a training session on the protection of personal data in the first half of 2019, which also includes specific aspects and examples relating to the correct delivery of reports"; the "preparation of a monitoring plan (so-called follow up) of the activities carried out by CDI staff in compliance with the GDPR, with specific checks on compliance with the procedure regarding the delivery of reports";

- with reference to the communication of violation of February 15, 2019, that "the insertion of the patient's report in the envelope relating to the other patient is attributed to a human error by one of the staff of the Imaging Diagnostics secretariat, belonging always to the administrative staff of the Customer Service, in charge of enveloping the reports before their delivery to the points (cash desks) for collection by the users concerned. The authorized person of the Diagnostics secretariat obviously made a mistake in reading the surname reported in the report and inserted it in the patient's envelope with the similar surname. Also in this case, CDI has taken initiatives to raise the awareness of the aforementioned personnel authorized to process the treatment at the Diagnostic Imaging Secretariat, sending a specific communication to raise awareness on the need to pay the utmost attention in the Bagging phase of the reports. Furthermore, by the end of the first half of 2019, the implementation of a control system by means of barcode reading was also planned at the Imaging Diagnostics secretariat in order to avoid errors even in the bagging phase of the reports ";

- with reference to the aforementioned events, it was highlighted that "they occurred despite the presence of suitable organizational, technical and safety safeguards aimed at preventing any anomalies (specific instructions on the procedures for managing and delivering reports, on the processing of personal data, further check such as the obligation to read with the scanner gun supplied, etc.). In this sense, to give an idea of the accidental nature of the events in question, it is useful to point out that the reports collected monthly by users at CDI are on average about 31,000. Compared to the overall volume of reports delivered monthly, the two cases described above therefore represent a very low percentage, equal to about 0.003% (taken individually on a monthly basis). In particular, the Customer Service staff assigned by CDI also to the management and delivery of the reports is about 40 employees, with the daily forecast of an adequate number of employees both at the points or cash desks for collecting the reports, and at the secretariat of the Diagnostic Imaging ";

- with reference to the communication of violation of 21 December 2018, that "from the verifications carried out by the same, it emerged that the start of production of the integration between the SW relating to the web portal and the SW for viewing Ebit images took place on 18/12/2017, and that, in the 45 days preceding the reported event, the cases in which the presence of an anomaly was found regarding the non-uniqueness of the identification code generated on different diagnostic equipment were 35 (out of a total about 27,000 diagnostic imaging exams managed in that period), with respect to which it was however possible to ascertain that there were no cases of viewing images of other patients, in addition to the one reported; on the same day, the image viewing function on the CDI web portal was temporarily blocked, pending completion of the analyzes and

carrying out corrective actions on a technical level; on 20.12, the correction to the malfunction was applied by Ebit, with the correct and complete configuration of the software countermeasure of the integration process aimed at preventing the display of images in the event of anomalies found in the related identification codes generated by the diagnostics and, subsequently adequate testing and verification activities, also in relation to the correction of the error that occurred in the reported case and to the further anomalies found, the online report viewing service was restored. Following the technical report sent by Ebit on 20.12, CDI invited a communication to the patient who submitted the complaint, providing the necessary clarifications on the case and on the measures taken to solve the problem, having confirmed the correctness of the report and the images of the examination carried out by the same reported on the CD-DVD, which can be collected at the CDI headquarters (given that, as emerged from the checks carried out, no problem had instead arisen within the system used by the radiologist who, at the time of the report, had correctly visualized the images to be reported of the respective patients, then transcribed on the CD-DVD "." It was an occasional and isolated episode, as, as confirmed by the technical checks carried out by the supplier, there were no other cases of visualization of images of other patients (although other anomalies were found, albeit in a rather limited number, 35). considering the total number of diagnostic imaging reports made available online, equal to approximately 27,000 in the 45 days preceding the reported event, the case in question represents a very low percentage of 0.13% ";

- with reference to the complaint submitted to the Guarantor, that the event "occurred exclusively within the ESF of the Lombardy Region, made available to users through the relevant website, and that, in relation to the processing of personal data to feed the ESF, CDI plays the role of owner of the processing of personal data and Lombardia Informatica S.p.A. (company subject to management and coordination by the Lombardy Region), that of data processor ". Specifically, as already highlighted in the previous note, following in-depth checks, it emerged that the event was caused by a technical error in the operation of the acceptance computer system used by CDI (a so-called "bug" that occurs only during 'execution), developed together with Accenture S.p.A. hereinafter also "Accenture"), which also takes care of its development and maintenance, as data processor. In particular, in the phase of acceptance of a patient under the agreement with the SSN, the system, in addition to consulting or creating the relative data in the CDI systems, also acquires (through web services) the regional one present in the IT system (SISS) of the Lombardy Region for the subsequent forwarding of the report to the ESF. In the present case, the IT system of acceptance of CDI, in carrying out this operation, due to the aforementioned operating error, has combined the regional personal data of the complainant acquired by the regional system, to the personal data relating to a

different person present on the CDI. This therefore entailed the aforementioned inclusion in the FSE of the complainant of the data relating to another user of CDI's health services. As mentioned, the event was caused by a technical error in the operation of the acceptance computer system impossible to detect during the development phase) which was in any case installed, configured and tested in order to guarantee an adequate level of safety for the risk connected to the treatment under consideration. We also inform you that, in light of the incident, the log files of the publications of the reports from 01.01.2016 to 20.01.2019 were examined and it was possible to highlight that, out of the 2,368,091 published reports, the aforementioned anomaly of the system involved only 62 reports thus having an incidence of 0.0026% (it should also be noted that a total of 48 patients are referred to, with respect to which it appears that only 7 reports, including the two reported by the complainant, were viewed atypical way). Such a low frequency of the error has prevented that, despite the program had been tested, validated and subject to scheduled maintenance, this anomaly was detected in advance ". As regards, then, the 62 events, including the 2 reported by the complainant, due to the same causes, a request for removal of the reports was sent to Lombardia Informatica which provided information regarding the number of reports actually displayed (see above) and proceeded with the cancellation ".

With a subsequent communication of January 28, 2020, the aforementioned Center renounced to be heard by the Authority regarding the aforementioned investigative proceedings.

2. Outcome of the preliminary investigation

Having taken note of what is represented by the Italian Diagnostic Center in the documentation in deeds and in the defense briefs, it is noted that:

1. the Regulation, in establishing a general prohibition 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 Article 12, Legislative Decree no. 179/2012, Prime Ministerial Decree no. 178/2015). The processing of personal data in question can be traced back to the cases indicated in art. 9, par. 2, lett. h) of the Regulations;

2. the material and technical errors described above have repeatedly determined the possibility that users of the Center could access the data relating to the health of other users; specifically, the reported event of 24 October 2018 involved one (1) interested party, that of 21 December 2018 thirty-five (35) interested, that of 15 February 2019 one (1) interested party and the

one subject to the aforementioned complaint sixty-two (62) interested.

3. Conclusions

In light of the aforementioned assessments, taking into account the statements made by the data controller during the investigation and considering that, unless the fact constitutes a more serious crime, anyone, in a proceeding before the Guarantor, falsely declares or certifies information o circumstances o produces false deeds or documents is liable pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the tasks or 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 initiation of the procedure, however, as none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the Italian Diagnostic Center in Milan under the terms set out in the motivation, for violation of Articles 5, par. 1, lett. a) and f), and 9 of the Regulations. This, also with reference to the Centre's failure to adopt technical and organizational measures aimed at effectively implementing the principles of data protection from the design stage, as well as guaranteeing a level of data security appropriate to the risk (see articles 25 and 32 of the Regulation).

In this context, considering, in any case, that the conduct has exhausted its effects, given that the Center has declared that the aforementioned technical error has been corrected and the reports have been correctly attributed to the subjects to which they refer, they do not resort the conditions for the adoption of the corrective measures pursuant to art. 58, par. 2, of the Regulation.

4. Adoption of the injunction order for the application of the pecuniary administrative sanction and ancillary sanctions (articles 58, par. 2, lett. I and 83 of the Regulation; art. 166, paragraph 7, of the Code).

The violation of articles 5, par. 1, lett. a) and f), and 9 of the Regulations, caused by the conduct carried out by the Italian Diagnostic Center in Milan, is subject to the application of a pecuniary administrative sanction pursuant to art. 83, paragraph 5, lett. a) of the Regulations.

It should be considered that 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).

The aforementioned administrative fine 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 light of the elements provided for in art. 85, par. 2, of the Regulation in relation to which it is noted that:

- the Authority in three of the four cases examined became aware of the event following the notifications of violation of personal data made by the same owner; an investigation procedure was instead initiated following the submission of a complaint by the interested party (Article 83, paragraph 2, letter h) of the Regulations);
- the processing of data carried out by the Italian Diagnostic Center subject to this provision concerns data suitable for detecting information on the health of various interested parties (overall 99) (Article 83, paragraph 2, letters a) and g) of the Regulation);
- the absence of voluntary elements on the part of the Italian Diagnostic Center in the causation of events (Article 83, paragraph 2, letter b) of the Regulation);
- the immediate taking charge of the problem followed by the identification of corrective and resolving solutions (art. 5, par. 2 and art. 83, par. 2, lett. c) and d) of the Regulations);
- the holder has demonstrated a high degree of cooperation (Article 83, paragraph 2, letters c), d) and f) of the Regulation).

Due to the aforementioned elements, assessed as a whole, also taking into account the phase of first application of the sanctioning provisions pursuant to art. 22, paragraph 13, of the d. lgs. 10/08/2018, n. 101, it is believed to determine the amount of the pecuniary sanction provided for by art. 83, par. 5, lett. a) of the Regulations, to the extent of € 50,000 (fifty thousand) for the violation of Articles 5, par. 1, lett. a) and f) and 9 of the Regulations as a pecuniary administrative sanction, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed 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 art. 16 of the Guarantor Regulation 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 is noted 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

declares the unlawfulness of the processing of personal data carried out by the Italian Diagnostic Center in Milan, for the violation of Articles 5, par. 1, lett. a) and f), and 9 of the Regulations in the terms set out in the motivation.

ORDER

pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, at the Italian Diagnostic Center in Milan, with registered office in Via Simone Saint Bon n. 20 - 20147 Milan - tax code and VAT number 01721030151, in the person of the pro-tempore legal representative, to pay the sum of 50,000 (fifty thousand) euros as a pecuniary administrative sanction for the violations indicated in this provision, according to the methods indicated in the annex, within 30 days from notification in 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 sanction imposed.

INJUNCES

to the aforementioned Italian Diagnostic Center in Milan, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 50,000 (fifty 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 law n. 689/1981.

HAS

pursuant to art. 166, paragraph 7, of the Code, the full publication of this provision on the website of the Guarantor and believes 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.

Pursuant to art. 78 of the Regulation, of art. 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, March 25, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei