[doc. web n. 9581069]

Injunction order against the Local Health Unit of Reggio Emilia - 11 March 2021

Record of measures

n. 92 of 11 March 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Giuseppe Stanzione, president, Prof. Ginevra Cerrina Feroni, vice president, Avv. Guido Scorza and dr. Agostino Ghiglia, 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");

HAVING REGARD to the “Guidelines 01/2021 on Examples regarding Data Breach Notification” adopted by the European Data Protection Committee on 14 January 2021;

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");

Having seen 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 operation of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web n. 1098801;

Rapporteur the lawyer Guido Scorza;

WHEREAS

1. The violation of personal data.

The Local Health Unit of Reggio Emilia (hereinafter the "Company") has notified the Guarantor of a breach of personal data, pursuant to art. 33 of the Regulation, in relation to an error in entering the date, in a batch of reports from 2010, which resulted in their association with bookings of different patients, made in 2019, with consequent communication to people other than those concerned. The event described, which involved eight people, originated in 2010, but the Company became aware of it on March 18, 2019.

In the same communication it was highlighted that the violation concerned identification data (such as surname, name, residence and tax code), contact data (telephone number), health data, relating to blood tests of the Diabetes Analysis Center of the Hospital of Montecchio (glycemia, cholesterol, urine, etc.) of the eight patients recalled.

The data controller has also declared that it has adopted technical and organizational measures aimed at preventing similar future violations such as the elimination of "references to booking numbers relating to subsequent years" (and) "the introduction into the unloading systems reports (SWAR and SWARI), a further check on the tax code associated with the report and the booking "(see communication of 21 March 2019).

2. The preliminary activity.

In relation to what was communicated by the Company, the Office, with deed of 25 July 2019, prot. n. 25764, initiated, pursuant to art. 166, paragraph 5, of the Code, with reference to the specific situations of illegality referred to therein, a procedure for the adoption of the measures referred to in art. 58, par. 2 of the Regulation, towards the same Company, inviting it 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, l. N. 689 of November 24, 1981).

In particular, the Office, in the aforementioned deed, has preliminarily represented that:

- in the health field, information on the state of health can only be communicated to the interested party and can be communicated to third parties only on the basis of a suitable legal basis or on the indication of the interested party himself, subject to the written delegation of the latter (art. 9 Regulation and art.84 of the Code in conjunction with art.22, paragraph 11, legislative decree 10 August 2018, n.101; see also general provision of 9 November 2005, available at www.gpdt. it, web doc. n. 1191411, deemed compatible with the aforementioned Regulation and with the provisions of decree n. 101/2018; see art. 22, paragraph 4, of the aforementioned legislative decree n. 101/2018);

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

That said, with the aforementioned act of 25 July 2019, the Office ascertained that the Company made a communication of data relating to the health of 8 patients to other patients in the absence of a suitable legal basis and, therefore, in violation of the basic principles of the treatment referred to in art. 5 and 9 of the Regulations.

With a note dated 23 August 2019, the Company sent its defense briefs, in which, in particular, it was specified that:

a) "the event that made the error evident occurred due to potential online access which took place between 14 and 18 March 2019, at n. 8 reports of routine blood tests, carried out in 2010, by 8 subjects other than those concerned. It is specified that access to the content of the reports has been ascertained only with respect to 2 of the aforementioned 8 cases ";

b) "it emerged that a set of reports generated in 2010, with a booking made at the end of 2009, incorrectly reported a booking number for the year 2019; consequently, these 2010 reports had been associated, in the download phase, with bookings of 2019 referring to interested parties other than those to which the 2010 reports refer ";

c) the Information Technology and Telematics Service "proceeded, through the current suppliers, to identify the origin of the incorrect attribution of reports and to structurally solve the problem, adopting the following precautions:

- Identifying and eliminating, where present, the links of the reports to booking numbers relating to years subsequent to that of the report originating the problem: for this purpose all the laboratory reports on the repository were analyzed and verified to analyze and eliminate the aforementioned links ;

- By introducing a further check of the correct association between the tax code contained in the report to be downloaded and the tax code on the two online download systems (SWAR and SWARI), already designed by design with verification of matching between the patient's tax code and booking number who is downloading the report, thus ensuring greater protection against potential erroneous attributions of booking numbers; no longer present, but the change was introduced as an additional protection and safety measure ";

d) the "Algorithm for association reports - booking-otp prior to the episode" worked according to the following steps: "The patient must enter his tax code (hereinafter CF) and his online report collection number (OTP) ; based on the match between the two previous data, the system verifies the existence of the corresponding reservation; based on the corresponding

reservation number, the system retrieves the PDFs of the reports and makes them available to the user.

Following the incident, the algorithm was changed to include an a posteriori check on the patient's CF: the patient must enter their CF and their online report collection number (OTP); based on the match between the two previous data, the system verifies the existence of the corresponding reservation; on the basis of the corresponding reservation number, the system retrieves the PDFs of the reports; for each report retrieved, the correspondence with the CF indicated by the patient himself is checked, and corresponding to the report withdrawal code. The reports are made available to the user ";

e) contacted the interested parties (i.e. the subjects to whom the 2010 reports incorrectly downloaded) referred, they "expressed appreciation for the correctness and transparency of the Administration, highlighting that they do not consider themselves harmed in the freedom or dignity of the disclosure of a data , in their own words, not excessively delicate even if of a particular nature, as well as dating back many years before ";

f) “the evaluation of the case made it possible to detect the precise duration of the violation which is attributable to a specific and very limited time, since the accesses lasted a few minutes each. (…) The online reporting system does not allow to certify that, with the exception of the 2 reporting persons, the other 6 recipients of the incorrect report have actually viewed the documents containing the data of the interested parties ";

g) "from a comparison of the numbering of bookings, which took place in 2009 and the reports generated in 2010, it was possible to infer that, due to a probable software design error, the system, within a series of bookings at the end of 2009, added to the booking number that began with no. 9, prefix 201, effectively generating a number similar to the current progressive one, year 2019 "but it is not possible to establish in which phase (booking transmission and report transmission) the error was generated";

h) "the detected error was blocked in less than 60 minutes and corrected in less than 2 hours from the report";

i) "with the exception of the 2 patients who reported the malfunction, the others may not even have realized the error, since the correctly assigned one was also visible in the download of the report";

j) "it is not currently possible to establish negligent conduct by the supplier of the booking and reporting software, in the absence of certain data, due to the replacement of the system and the number of years that have elapsed";

k) "The Company has prepared, since the entry into force of the European Regulation, a capillary corporate training plan customized to the various professional roles. In 2018 alone, at least 8 sessions / events dedicated to the categories of

professionals were held: Delegates for treatment, Committee and Departmental and District Representatives. Specific frontal events were organized for the different categories of operators (approximately 20 training events in June 2019) ".

In relation to the measures adopted to mitigate the effects of the violation for the data subjects, the measures described in the communication containing the notification of personal data violation were again illustrated and it was highlighted that: "the current CUP management system (Booking System ) sends the reservation to the LIS (Laboratory System), which in the reporting phase sends the report with the reservation number to the CDR (Clinical Data Repository). The report retrieval system for delivery to the patient retrieves the report from the CDR by querying the reservation number and time, after the redundant control system, also the correspondence of the tax code of the report with the tax code of the reservation ", specifying that" all maintenance and development activities on the software under management are currently tracked on a specific repository, from the activation of the order to testing. All transmissions of health data on the systems involved in the path in question take place in secure mode (encrypted protocols) both to the outside (internet) and to internal communications. Each operation of the online access path to the reports described is subject to tracking ".

On October 31, 2019, the hearing requested by the data controller was held at the Guarantor's Offices, during which it was further represented that the IT measures adopted to solve the problem were "subjected to subsequent tests that made it possible to verify the robustness of the aforementioned measures adopted ".

The Company therefore asked "on the basis of the foregoing to proceed with the filing of the administrative procedure and, in the alternative, without acknowledging the validity of the complaints, the application of a penalty in the smallest amount possible".

3. Outcome of the preliminary investigation

Given that, unless the fact constitutes a more serious crime, whoever, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces false documents or documents, is liable pursuant to art. 168 of the Code ("False declarations to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor"), following the examination of the documentation acquired as well as the declarations made to the Authority during the procedure, that:

1. although the violation began in 2010, in order to determine the applicable law, in terms of time, the principle of legality referred to in art. 1, paragraph 2, of the l. n. 689/1981, which states that "Laws that provide for administrative sanctions are

applied only in the cases and times considered in them". This determines the obligation to take into consideration the provisions in force at the time of the violation committed, which in the case in question - given the permanent nature of the alleged offense - must be identified at the time of cessation of the unlawful omissive conduct, which occurred after the date of 25 May 2018 in which the Regulation became applicable. In fact, from the preliminary investigation it emerged that the event from which the unlawful communication of health data originated took place in 2010, but the Company became aware of it on March 18, 2019 and in the same year. declared that it had removed its effects by adopting the technical and organizational measures aimed at preventing similar future violations;

2. the Company has made a communication of data relating to health in the absence of a suitable legal basis and, in the matter of personal data security, has failed to adopt technical and organizational measures to ensure a level of security appropriate to the risk (art. . 5, 9 and 32 of the Regulation).

4. Conclusions

In light of the aforementioned assessments, taking into account the statements made during the investigation, it is noted that the elements provided by the data controller in the defense briefs and during the hearing, albeit worthy of consideration - given the detail and appropriateness of the explanations provided, in relation to each element indicated in art. 83, par. 2, of the Regulation - do not allow the findings notified by the Office to be overcome with the act of initiating the procedure, however, 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 Local Health Unit of Reggio Emilia is noted, in the terms set out in the motivation, in violation of Articles 5 and 9 of the Regulations.

Consequently, regardless of the notification of the breach of personal data made by the data controller, in compliance with the obligation under art. 33 of the Regulation, the profiles of illegality of the processing detected in the present case, however, require the intervention of this Authority.

In this context, considering, in any case, that the conduct has exhausted its effects and that assurances have been provided regarding the technical measures adopted in order to avoid the repetition of the error that occurred, also verified in relation to their effectiveness, the conditions are met 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 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 and 9 of the Regulations, by the Local Health Unit of Reggio Emilia, is subject to the application of the pecuniary administrative sanction pursuant to art. 83, par. 5, of the Regulation.

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. 83, par. 2, of the Regulation in relation to which it is noted that:

1. the Authority became aware of the violation following the notification made in compliance with the terms of the law by the data controller who informed the interested parties of the incident; and no complaints or reports have been received to the Guarantor on the incident (Article 83, paragraph 2, letters a) and h) of the Regulations);

2. the problem was immediately taken over by the Company Information Technology and Telematics Service, promptly suspending the report download system and correcting the problem encountered by identifying solutions subjected to subsequent tests (Article 83, par. 2, letter c) of the Regulation);

3. There are no previous relevant violations committed by the data controller nor have any measures previously been ordered pursuant to art. 58 of the Regulations (Article 83, par. 2, lett. E) and i) of the Regulations);

4. the Company collaborated with the Authority during the investigation and this proceeding (Article 83, paragraph 2, letter f) of the Regulations).

Due to the aforementioned elements, assessed as a whole, 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 € 9,000.00 (nine thousand) for the violation of Articles 5 and 9 of the Regulation 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 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 Local Health Unit of Reggio Emilia, for the violation of art. 5, par. 1, lett. 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, to the Local Health Unit of Reggio Emilia with registered office in Reggio Emilia, in via Amendola 2 - VAT number 01598570354, in the person of the pro-tempore legal representative, to pay the sum of € 9,000.00 (nine thousand ) as a pecuniary administrative sanction for the violations indicated in this provision, according to the methods indicated in the annex, within 30 days from the notification of 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 Company, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 9,000.00 (nine 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

- 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, as well as by 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 11, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei