[doc. web n. 9746448]

Injunction order against the Northern Milan Territorial Social Healthcare Company - January 27, 2022

Record of measures

n. 34 of January 27, 2022

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 Dr. 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, bearing 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 regarding the processing of personal data, as well as 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 the Guarantor's 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 operation of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web n. 1098801;

Rapporteur Prof. Ginevra Cerrina Feroni;

WHEREAS

1. The preliminary activity.

A complaint was received by the Guarantor in which an interested party represented that in March 2021, by accessing the

website of the territorial social health company (hereinafter ASST) North of Milan to book a health service (buffer for the detection of the Sars virus Cov 2), found that the booking service was carried out on an "http" (hypertext transfer protocol) network protocol and that, by removing the "Reservation.php" extension from the address of the aforementioned Company's website, it was possible access the unencrypted information relating to some ASST patients who had joined the 2020/2021 influenza vaccination campaign and in particular the following data: name, surname, social security number, telephone numbers, place of booking and administration of the flu vaccine.

Following what has been reported, the Office found the absence of the files indicated by the complainant on the aforementioned website, as well as the unreachability of the web pages indicated by the same (with the exception of the one relating to the reservation of tampons for the search for SARS- CoV-2) and ascertained that the "http" network protocol was used for the aforementioned site and that an outdated basic software with characteristics that could compromise confidentiality and integrity was used on the server hosting the same of the data processed there.

In relation to the findings, the Office requested information from the ASST north of Milan (notes of 7.4.2021, prot. No. 18256 and of 7.6.2021, prot. No. 30975), which provided feedback with the notes of 23 April 2021 (prot. n.12788), of 22.6.2021 (prot. n.18660), of 28.6.2021 (prot. n. 18977) and of 8 July 2021 (prot. n. 19998) ) in which it was, in particular, represented that:

"It is our duty to emphasize first of all the context (Article 32, C.I of the GDPR) in which the data processing by ASST Nord Milano took place and the event subject to reporting took place, ie an emergency period that, for more than a year now, it has been putting a strain on both the resilience of the health system (hospital and territorial) as a whole ";

"The site was developed with" phpMyAdmin 2.10.3 "and was created in three working days, to address the emerging business needs regarding the booking of flu vaccine sessions, replacing an overly burdensome management via email" "subsequently it is the section relating to the reservation of Swabs for the research of Covid-19 under solvency was also developed ";

“For both the Swabs and the vaccinations, the name, surname, tax code and telephone number were collected, associated with the time and place where the service would take place. These data represent the minimum "set" to correctly identify a person and to manage "and" any communication of appointment displacement generated by the supplying company ";

"The SIA Manager specified that, precisely being well aware of the age of the operating systems adopted - the only ones in any case able to respond at that time to the urgent needs of public interest connected to the management of serious threats to health, even of a cross-border nature - the installation and testing of the new software platform, based on "phpMyAdmin

7.3.10", were subsequently planned;

“The tests for the software migration, which also led to all the necessary updates of the code due to the new development platform, were concluded on Thursday 18.3.2021”;

“It was deliberately chosen not to migrate the system on Friday, to avoid leaving a newly migrated system unattended for a whole weekend and which could have" youth defects "(bugs not found in the test cycles)";

“At 14.00 on Monday 22 March 2021, the migration took place and all the problems highlighted in the email of Mr. XX at 01.02 of the same day have been solved. It therefore appears unlikely that the same, after 48 hours following the sending of the email, could have accessed the data he claims to have come into possession, which is unfortunately possible until 2.00 pm on 22.3.2021 ";

“A program component is also being written to historicize bookings relating to a past time on a system not exposed to the public in order to minimize the impact of a new possible intrusion”;

"Pursuant to art. 34, paragraph 3, lett. b) of Regulation (EU) 2016/679, the communication to the interested parties is not required (the "1782 lines (not all valid) of citizens of the ASST area who have joined the flu vaccination campaign" mentioned by Mr. XX in the communication to the Guarantor) as the Data Controller has subsequently adopted measures aimed at avoiding the occurrence of a high risk for the rights and freedoms of the interested parties themselves ";

"When your Dear Authority on 7 April u.s. reported the statement with which the complainant claimed instead of having had access to the data after 48 hours (from 1 am on 22 March), the SIA Manager rightly pointed out that it was not possible that this violation had occurred, because after 48 hours that database was no longer accessible, as it was removed from the site together with the start-up of the new software (which no longer contained the database in question), therefore from 14.00 on 22 March; the Guarantor Authority itself, connecting remotely, did not find any trace of the data in question; since there was no evidence of a violation, there were no conditions for proceeding with notifications to the Guarantor and to the interested parties ";

"After the aforementioned reply to the Guarantor Authority on 23 April, the Offices concerned investigated two aspects: - whether or not there were the conditions for a legal action against the whistleblower for the crime referred to in Article 615 ter of Criminal Code ("Unauthorized access to a computer or telecommunications system protected by security measures"); to consider also that Mr. XX used in XX; - the reasons why the complainant could have declared that he had viewed the data -

fortunately, not particular "- of about 1772 people after 48 hours, when this was not objectively possible";

"Given the above, and in view of the Authority's request for further clarifications on 7 June last year, a second investigation was in fact carried out on access to data, which allowed the SIA Manager on 15 June to communicate that around 3.00 am on March 22 there was a probable second access to the database (the details are present in the aforementioned Report). To date, however, we have no objective evidence that the complainant actually consulted the database at about 3.00 ";

"The news of the probable intrusion was therefore treated as an accident from scratch, and notification was made pursuant to Article 33 of Regulation (EU) 2016/679, within 72 hours from when I personally became aware of it (our prot. no. 18309 of 18.06.2021) ".

As stated in the documents, on 18 June 2021 the ASST, pursuant to art. 33 of the Regulation, sent to the Guarantor the notification of personal data breach, concerning access by a third party to the data of over 1700 patients who have joined the 2020/2021 flu vaccination campaign. The aforementioned Company declared that on June 16, 2021 it became aware of the violation that took place on March 22, 2021 "following research carried out in relation to the proceeding" initiated by the undersigned Department (see note of June 18, 2021, section C points 2 and 3 and report of the Head of Corporate Information Systems (SIA) dated 17/06/2021 attached to the notification).

In the aforementioned notification, the ASST represented that, taking note of the XX, [...] in which - verbatim, under its own responsibility - he writes: "I proceeded to destroy the local copy without ever disseminating or using it", it decided not to prepare any communication to users "(see note of 18 June 2021 section G point 1).

As regards the measures to ensure the security of the processing in place at the time of the violation of the personal data subject to notification, the ASST stated that:

- "the technical measures adopted up to 2.00 pm on 22.3.2021, with reference to the integrity, security and confidentiality of the data, were: - Backup twice a day of the registered bookings, with historical depth of 15 calendar days and with data saved on another device not accessible from the external network (behind a firewall) - Protected physical access to the server room - System administrative users issued only to SIA technical personnel - Presence of a "cold" backup server that can be activated in 20 minutes from the unavailability of the main system . To these measures, from 2.00 pm on 22.3.2021, the Block of all pages not related to the service and of the backdoors notes on the new version has been added. to the public reservations relating to a past time in order to minimize the impact of a new possible intrusion ";

- "The Company, as already stated, was not aware of the fact that" unauthorized "access to its software had occurred, carried out with non" common "methods and skills, such as to highlight the health data present in the software . The awareness of the possible vulnerability of the site - temporarily tolerated for the reasons explained, unfortunately given the current health emergency situation - had however already given rise to the necessary actions to restore its safety "(see note of 23 April 2021).

As regards the measures adopted to prevent similar violations in the future, the ASST stated that "starting from 30/3/2021 a tracking and log function was activated, not present on the previous system, which allows to analyze the status of any intrusion attempts and their frequency and evolution [...] From 21/4/2021 the https protocol (port 443) was then introduced in place of the previous http (port 80), in order to make transactions even more secure "(See SIA report, cit.).

In relation to what emerged from the documentation in the file, the Office, in ordering the meeting of the investigative proceedings initiated following the aforementioned complaint and the notification of violation made by the ASST north of Milan, notified it, 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 Regulations, inviting the aforementioned owner 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 no. . 689 of 11/24/1981) (note of November 2, 2021, prot. No. 54617).

In this act, the Office, in taking note of the actions taken by the ASST to overcome the criticalities that emerged during the procedure, considered that the processing of personal data in question was carried out in a manner that did not comply with the principles of " integrity and confidentiality "(Article 5, paragraph 1, letter f) of the Regulations), failing to implement, from the design of the website / web service, technical and organizational measures suitable to guarantee a level of security adequate to the risk (articles 25 and 32 of the Regulation). The aforementioned deed also represented the delay in the notification of violation to the Authority with respect to the provisions of art. 33 of the Regulation.

With a note dated 25 November 2021, the ASST north of Milan sent its defense briefs, in which the "peculiar" context "(...) in which the booking system subject to the report was put in place was reiterated, that is a situation of overt emergency linked to the pandemic "," the demonstrated desire to apply ever greater security measures, which, as clarified, were designed regardless of the report received "and" the necessary balance of interests between the urgency to adopt efficient and immediate solutions for citizens, aimed at ensuring the continuity of the flu vaccination service with all the related health

consequences, and the security measures objectively applicable at that juncture ".

2. Outcome of the preliminary investigation.

Having taken note of what is represented by the ASST north of Milan in the documentation in deeds and in the defense briefs, it is noted that:

pursuant to the Regulation, "data relating to health" are considered personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information relating to his state of health (Article 4, par . 1, no. 15, of the Regulation). Recital no. 35 of the Regulation then specifies that the data relating to health "include information on the natural person collected during his registration in order to receive health care services"; "A specific number, symbol or element attributed to a natural person to uniquely identify him for health purposes";

the Regulation provides that personal data are "processed in such a way as to guarantee adequate security (...) including protection, by means of adequate 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 Regulations). The Regulation also provides that the data controller, taking into account the state of the art and the implementation costs, as well as the nature, object, context and purposes of the processing, as well as the risk of varying probability and severity for rights and freedoms of natural persons, must put in place adequate technical and organizational measures to guarantee a level of security appropriate to the risk, which include, among others, where appropriate, "the encryption of personal data" (Article 32 of Regulation);

based on the principle of "data protection from design", pursuant to art. 25, par. 1, of the Regulation, the data controller, taking into account the state of the art and the implementation costs, as well as the nature, scope of application, context and purposes of the processing, as well as risks having different probabilities and gravity for the rights and freedoms of natural persons constituted by the processing, both at the time of determining the means of processing and at the time of the processing itself, must put in place adequate technical and organizational measures, aimed at effectively implementing the protection principles of the data and to integrate the necessary guarantees into the processing in order to meet the requirements of the Regulation and protect the rights of the data subjects;

the Regulation establishes that "in the event of a violation of personal data, the data controller notifies the violation to the competent supervisory authority pursuant to Article 55 without undue delay and, where possible, within 72 hours from the time

it came aware, unless it is unlikely that the breach of personal data presents a risk to the rights and freedoms of individuals. If the notification to the supervisory authority is not made within 72 hours, it is accompanied by the reasons for the delay "(art. 33, par. 1). In this regard, the "Guidelines on the notification of personal data breaches pursuant to Regulation (EU) 2016/679" of the Article 29 Data Protection Working Group of 3 October 2017, as amended and last adopted on 6 February 2018 and endorsed by the European Data Protection Committee on 25 May 2018 (hereinafter "Guidelines"), establish that "the data controller must be considered" aware "when it is reasonably certain that a security incident that led to the compromise of personal data. […] The data controller is therefore required to take the necessary measures to ensure that he is "aware" of any violations in a timely manner so as to be able to take the appropriate measures "(par. II.A.2). In addition, the Guidelines provide that "if a person, communications organization or other source informs the data controller of a potential breach or if he himself detects a security incident, the data controller may carry out a brief investigation to determine if the violation actually occurred. During the investigation period, the data controller cannot be considered “in the know. However, the initial investigation is expected to begin as soon as possible and establish with reasonable certainty whether a violation has occurred; a more detailed investigation can then follow. After the controller becomes aware of a notifiable breach, it must be notified without undue delay and, where possible, within 72 hours. During this period, the data controller should assess the probable risk for natural persons in order to establish whether the requirement for notification is met and what actions are necessary to deal with the breach "(par. II.A.2);

the urgent provisions adopted in recent months provide for emergency interventions that involve the processing of data and which are the result of a delicate balance between public health needs and those relating to the protection of personal data, in compliance with the provisions of Regulation for the pursuit of reasons of public interest in the public health sectors (see Article 9, paragraph 1, letter i)). It is obviously understood that the processing of personal data connected to the management of the aforementioned health emergency must be carried out in compliance with the current legislation on the protection of personal data and, in particular, with the principles applicable to the processing, pursuant to art. 5 and 25, par. 2, of the Regulations, in part referred to above;

the aforementioned urgent legislation did not derogate from the principles of confidentiality and data integrity (Article 5, paragraph 1, letter f) of the Regulation), of "data protection by design) (Article 25 of the Regulation) and the provisions on the protection of personal data relating to the security of processing (Article 32 of the Regulation) and the violation of personal data

(Article 33 of the Regulation);

the aforementioned violation of personal data, as declared in documents by the ASST north of Milan, was brought to the attention of the same with the request for information from the Office of the Guarantor of April 7, 2021, during the preliminary investigation. In view of this, it is noted that the same Company notified the violation only on 18 June 2021, without giving the reasons for the delay. The elements provided in the aforementioned request for information were such as to allow the holder to be “reasonably certain that a security incident has occurred which led to the compromise of personal data” (see the aforementioned Guidelines, spec. Par. II. A.2), also taking into account that the aforementioned request expressly requested "the assessments carried out in relation to the risks to the rights and freedoms for the interested parties deriving from the incident subject to reporting, also in order to verify the existence of the conditions for the notification of the violation of personal data to the Authority and, if necessary, the communication of the same to the interested parties involved (articles 33 and 34 of the Regulation) "and, subsequently, the" more detailed information regarding the reasons for of which the notification of violation of personal data has not been made (Article 33 of the Regulation) and the communication of the same to the interested parties (Article 34) ". The aforementioned delay in notifying the violation of personal data integrates the details of a violation of the obligations referred to in art. 33 of the Regulation;

as documented in the documents, the personal data of the patients who joined the 2020/2021 flu vaccination campaign, stored on the server that provided the "light" booking service for the flu vaccination ", were indexed and freely traceable online with the 'use of common web search engines. Therefore, anyone, carrying out a search with a common search engine, could have access to the files available at the URLs http://2.228.136.235/vacEage/agenda.csv and http://2.228.136.235/vacEage/agenda2020.csv. This was due to the absence of a computer authentication system that should have limited access to authorized persons with appropriate authentication credentials only. Considering that the online service was exposed to the aforementioned risks of cyber attacks and taking into account the absence of an IT authentication system, the measures adopted by the ASST north of Milan do not comply with the provisions of art. 5, par. 1, lett. f), and art. 32, par. 1, of the Regulation.

in the state of the art, the use of cryptographic techniques is one of the measures commonly adopted to protect, in particular, the personal data of users of an online service during their transmission over the Internet. From the assessment carried out on the basis of the elements acquired and the facts that emerged as a result of the investigation, it appears that access to the web

service for booking tampons for the search for SARS-CoV-2 took place in an unsafe manner, through the network protocol "http" (hypertext transfer protocol). This protocol, in fact, does not guarantee the confidentiality and integrity of the data exchanged between the user's browser and the server that hosts the Company's website, and does not allow users to verify the authenticity of the site displayed. Taking into account the nature, object and purpose of the processing, as well as the risks affecting the data and the possible "cloning" of the website in question for the acquisition of data transmitted for illegal purposes, the solution adopted by ASST nord of Milan cannot be considered a suitable technical measure to guarantee an adequate level of security for the risks presented by the processing, which involves the transmission of data, including health related data, on a public communications network. Failure to use cryptographic techniques to transport data therefore constitutes a violation of art. 5, par. 1, lett. f), and art. 32 of the Regulation, which, moreover, in par. 1, lett. a), expressly identifies data encryption as one of the possible security measures suitable for guaranteeing a level of security appropriate to the risk (on this point, see also recital no. 83 of the Regulation in the part in which it provides that "the owner of the processing […] should assess the risks inherent in the processing and implement measures to limit those risks, such as encryption "). The ASST north of Milan, in fact, should have put in place, right from the design of its website / web service, adequate technical and organizational measures, aimed at effectively implementing the principles of data protection, including the principle of " integrity and confidentiality ", adopting a secure network protocol, such as the aforementioned" https "protocol (hypertext transfer protocol over secure socket layer), within the context of the website / web service subject of the complaint.

3. Conclusions.

In light of the aforementioned assessments, taking into account the statements made by the owner 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 news or circumstances o produces false deeds or documents and 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 ASST north of Milan, in the terms set out in the motivation, is noted, in violation of Articles 5, paragraph 1, lett. f), 25, 32 and 33 of the Regulation.

In this context, it being understood that the complainant has declared that he has destroyed a copy of the documentation he

has accessed, considering, in any case, that the conduct has exhausted its effects, given that the ASST has chosen a new software platform, introduced the tracking function, as well as adopted a secure communication protocol ("https"), 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, paragraph 2, letter i), and 83 of the Regulations; art. 166, paragraph 7, of the Code).

The violation of articles 5, paragraph 1, lett. f), 25, 32 and 33 of the Regulations, caused by the conduct put in place by the ASST north of Milan, is subject to the application of a pecuniary administrative sanction pursuant to art. 83, par. 4 and 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. 85, par. 2, of the Regulation in relation to which it is noted that:

the Authority became aware of the event following a complaint; on the same facts, the owner subsequently submitted a notification of personal data breach (Article 83, paragraph 2, letter h), of the Regulation);

the processing carried out by the ASST concerns particular categories of data such as those suitable for detecting information on the health of a significant number of data subjects (over 1700) (Article 83, paragraph 2, letters a) and g), of the Regulation);

the ASST has demonstrated a high degree of cooperation by working to introduce, even in the context of the emergency context - measures suitable for overcoming the findings expressed by the Office with the act of initiating the sanctioning procedure (Article 83, par. , letters c), d) and f), of the Regulation);

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 20,000 (twenty thousand) for the violation of Articles

5, paragraph 1, lett. f), 25, 32 and 33 of the Regulations or, as a withholding administrative fine, 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 by 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 Northern Milan Territorial Healthcare Company for the violation of Articles 5, paragraph 1, lett. f), 25, 32 and 33 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 Social Healthcare Company North of Milan, tax code 09320420962, in the person of the pro-tempore legal representative, to pay the sum of € 20,000 (twenty thousand) as a pecuniary administrative sanction for the violations indicated in this provision ; 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 € 20,000 (twenty 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 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, 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, January 27, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Cerrina Feroni

THE SECRETARY GENERAL

Mattei