[doc. web n. 9742435]

Injunction order against ASL Latina - December 16, 2021

Record of measures

n. 436 of December 16, 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, Professor Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, members and dr. Claudio Filippi, Deputy Secretary General;

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

Speaker Dr. Agostino Ghiglia;

WHEREAS

1. Notification of infringement and reporting

On the 20th, the ASL Latina, with registered office in Latina, V.le Pierluigi Nervi - Tax Code: 01684950593, (hereinafter the

"Healthcare Company") sent this Authority a "preliminary" notification of data breach personal, pursuant to art. 33 of the Regulation, subsequently integrated with a note of the XX.

In the act of notification, the health company represented that the violation had as its object the erroneous transmission to an unauthorized third party - by certified mail - of no. 2 documents containing, respectively, personal data and data relating to the health of other interested parties.

In particular, the Healthcare Company stated that "during the scanning of some documents concerning an assessment by the Prevention and Safety Service in the Workplaces and for which an application for access was presented by a legitimate subject external to the organization ASL, have been acquired, involuntarily, nr. two documents, not related to the access request. Of the two acts, one is inherent in the description of nr. two cases of positivity to Covid 19 and the other is related to a data request from the UOC Bilancio of the ASL, from which public data are deduced such as: the email addresses of nr. 3 ASL workers with institutional domain of the entity (___@ausl.latina.it) and internal telephone numbers of the offices to which the aforementioned workers belong ".

On the same occasion, it was also specified that "in order to contain the risk of infringing the fundamental rights and freedoms of the interested parties involved in the violation, through the Prevention Department, the Data Controller / ASL took action and requested the collaboration of the third party not authorized to process the personal data that is the subject of the violation which it has come into possession. In particular, the third party was required to destroy the documents received erroneously and containing the personal data in question and, therefore, to maintain the confidentiality of the information that he accidentally became aware of ".

According to what was declared by the Healthcare Company, "the violation occurred on 8.3.2021 and the department involved became aware of it on the same day, following a message sent by certified e-mail, by the third party who had erroneously received documentation containing personal data relating to other users. The department, due to the many activities related to the ongoing emergency management (vaccinations, tracking, etc.), communicated the event late (on XX date) to the privacy office. The privacy office is responsible for managing data breaches, as per company procedure. The data subject to violation are personal data (name, surname, sex, date of birth, place of birth, tax code); contact details (mobile phone number); health data ".

The Healthcare Company has also declared that it envisages the launch of "an additional information / training course,

consistent with the current emergency period and with the security measures adopted to contain the spread of the pandemic. In order to guarantee the processing of personal data inspired by the principles of Article 5 of EU Regulation 2016/679, the aforementioned path will aim to sensitize all company personnel in the correct observation of sector legislation, as well as the procedures implemented by the company in adherence to the principle of accountability. The entity / owner has envisaged the adoption of a secure printing system, to be activated where possible in correspondence with the printing equipment shared by several offices / workers and which provides for the insertion of a personal code to proceed with printing the generated document ".

Subsequently, in relation to the matter illustrated above, this Authority received a report from the person who had filed a request for access to the documents to the Latina ASL and received from the latter erroneously, in response, also the aforementioned documentation. In this report (note XX) what highlighted by the same health authority was confirmed.

2. The preliminary activity

Taking into account that the violation described with the notification made by the Healthcare Company pursuant to art. 33 of the Regulation concerns the same object of the proceeding initiated following the report, made on XX, against the same data controller, the two investigative proceedings were brought together and dealt with at the same time pursuant to art. 10, paragraph 4, of the “Regulation no. 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 "[Doc. web 9107633].

Having said this, on the basis of what is represented by the data controller in the act of notification of violation and what emerged from the report received from the Guarantor, as well as subsequent evaluations, the Office, with act of the XX (prot. No. XX), has notified the Healthcare Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in art. 58, par. 2, of the Regulation.

In particular, the Office, with the aforementioned deed, held that the ASL Latina, as data controller, by sending the n. 2 documents cited above, of which “one (…) inherent in the description of nr. two cases of positivity to Covid 19 and the other (…) relating to a data request from the UOC Bilancio of the ASL, from which public data are deduced such as: the email addresses of nr. 3 ASL workers with institutional domain of the entity (___@ausl.latina.it) and internal telephone numbers of the offices to which the aforementioned workers belong ", containing personal and health data to a third party not authorized to receive them, carried out a communication of personal and health-related data in the absence of a suitable legal basis and,

therefore, in violation of Articles 6 and 9 of the Regulation, the principle of integrity and confidentiality of data (Article 5, paragraph 1, letter f) and art. 2-ter of the Code. In relation to this, the Office has also invited the data controller 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 art. 18, paragraph 1, by law no. 689 of 11/24/1981).

With a note of the XX (prot. No. XX), the Healthcare Company presented a defense brief, in which, among other things, it highlighted that:

- “With respect to the violation event (…) the 2 human resources (specifically a doctor and an administrative employee) were identified who accidentally committed the error as represented by the Prevention Department in the communication of the XX prot. n. XX ";

- “the Data Controller / ASL has activated and requested the collaboration of the third party not authorized to process the personal data which is the subject of the violation which it has come into possession. In particular, the third party was required to destroy the documents received erroneously and containing the personal data in question and, therefore, to maintain the confidentiality of the information that he accidentally became aware of. Specifically, (...) the third party was sent no. 2 communications dated XX and XX (…). (...) In this context, the reliability of the unauthorized third party, the sole recipient of personal data, was assessed and this in consideration of the behavior assumed by the same to promptly inform the Data Controller / ASL about the receipt of irrelevant personal information compared to the request made. This element further reduced the level of risk for the interested parties involved. On the part of the Data Controller / ASL, acknowledgment of the report of the incident also made to the Guarantor Authority, strengthens the assessment of the reliability of the third party, reasonably leading to believe that the same has not undertaken and is not determined to undertake actions detrimental to the rights and freedoms of the interested parties that may result in prejudice for the same ";

- "Following the verification of the violation by the Guarantor Authority and a new risk assessment launched, this Data Controller, in collaboration with the corporate privacy team, the DPO and through the Department involved, reiterated to the third party the request for destruction of the personal data and respect for the confidentiality of personal information of which he has become aware, with the warning that failure to comply with these instructions will constitute, against him, a hypothesis of liability for violation ";

- "Of the two workers / persons authorized for the treatment in question: a) one, in the year 2020 and, in particular in February,

participated in a training day in line with the programming and planning of the training course previously organized according to business objectives. (...); b) the other has not yet participated in a specific training course in the classroom, as he was hired in November 2020. (...) In any case, it is represented that both workers have received instructions to perform the treatment of personal data in a secure manner, in compliance with the employment contract and the corporate code of conduct and, in general, in compliance with the laws of the sector ";

- "In the last reference period, (...) the Data Controller, (...) activated the" Procedure on the management of Personal Data Breaches - "Data Breach" (attachment no. 13), in order to undertake the process management of the violation and consequently carry out the appropriate formalities ";

- "As soon as the containment measures of the pandemic allow it, or in any case in FAD mode, it is the objective of the Company, provided for in the company Training Plan, to start a training course also for the current year. The Company, in fact, in compliance with the applicable European and national legislation, the guidelines, the rulings of the Guarantor Authority and in adherence to the specific complex organizational context which at that historical moment is heavily involved at an operational level in the management of the multiple health aspects of the pandemic crisis in progress, is always aimed at continuous improvement and raising awareness of the organization as a whole: attention paid to the protection of individuals, also with particular regard to the processing of personal data required in carrying out the activities / services provided " ;

- "The Data Controller (...) confirms the use of a secure printing system in correspondence with the shared printer, specifically, at the office of the Department involved, which requires the insertion of a personal code to proceed with the printing of the generated document. The adoption of this measure will be strengthened, where technically possible, at the various operating units that have printing equipment shared by several offices / workers ";

- "With regard to the description of the events, it is necessary to highlight the reference context: the third party has submitted a request for access to administrative documents at the Prevention Department, a structure indicated by the Health Plan, among other things, for the pandemic emergency in progress . The Structure, although overloaded by the emergency (planning and carrying out swabs, Covid vaccinations, tracing operations, etc.), however, continued to manage other ordinary activities as well. It must also be considered, in the general context of the Local Health Authority, the climate of organizational difficulty that the administrative staff is experiencing due to the management of the pandemic which has determined, especially in the Department, the need to face the emergency in progress through recourse to extraordinary measures such as: smartworking,

with consequent reduction of staff in attendance, recourse to human resources hired on a fixed-term basis, etc ";

- "In relation to the epidemiological state of emergency from Covid-19, it should be specified that the personal data subject to the violation even though they concern a state of health (Covid-19 infection), at the time of the violation and in the reference context (Department of Prevention ASL), have been processed for public health reasons and in particular for the purpose of containing / controlling the pandemic and not for purposes related to the care of the interested parties (e.g. diagnosis, assistance, therapy). It is also specified that the Prevention Department, already at the time of the supplementary notification, was aware of the negativization by the virus of the two users involved in the violation. It follows that for the data subjects there has not existed and does not exist a health situation known to third parties that could cause them material or immaterial damage, especially in terms of actual and concrete prejudice, compared to personal situations that provide for limitations of freedom or compliance with restrictive behavior. From the assessment of the risks for the case in question and in relation to the impact on the rights and freedoms of individuals, no high risk emerged, such as to proceed with communication to the interested parties ".

3. Outcome of the preliminary investigation

Having taken note of what is represented and documented during the investigation procedure by the Healthcare Company, first with the acts of notification of violation and, subsequently, with the defense brief produced following the act notified, pursuant to art. 166, by the Authority, it is noted that:

1. the Regulation provides that the processing of personal data is lawful only if and to the extent that one of the conditions provided for by art. 6 of the same Regulation;

2. 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 subject to written authorization from the interested party (Article 9 of the Regulation and Article 84 of the Code in conjunction with art.22, paragraph 11, legislative decree 10th August 2018, n.101);

3. the data controller is, in any case, required to comply with the principles of data protection, including that of "integrity and confidentiality", according to which personal data must be "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 "(Article 5, paragraph 1, letter f) of the Regulation ).

The health company, in its defense, reiterated that the illegal communication of data occurred due to a human error in the scanning phase of the documentation. This Company also stated that, as soon as the recipient of the aforementioned documents became aware of the incident, it immediately requested the recipient to ensure the confidentiality and destroy the documentation received and has adopted technical and organizational measures and undertaken actions to improve the working procedures. aimed at strengthening the guarantees placed to protect the protection of personal data.

4. Conclusions

In light of the aforementioned assessments, taking into account the statements made by the data controller during the investigation □ the truthfulness of which one may be called to answer pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor" findings notified by the Office with the act of initiating the procedure, since none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

For these reasons, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by the Latina ASL is noted. In particular, one of the two documents transmitted to the third party not authorized to receive them, reports data relating to two interested positive results at Covid 19, processed by the Healthcare Company for the purpose of containing and controlling the pandemic; another document concerns an internal note of the UOC Budget of the Healthcare Company, from which the telephone numbers of n. 3 employees of the same health company, internal to the offices to which these employees belong, who are not public as they are not found, at present, on the corporate institutional website for purposes referred to in legislative decree n. 33/2013. The communication of the aforementioned personal and health data therefore took place in the absence of the legal conditions provided for by the legislation for the protection of personal data and, therefore, in violation of Articles 6 and 9 of the Regulation, as well as the basic principles referred to in art. 5, par. 1, lett. f), of the same Regulation.

The violation of the aforementioned provisions makes it applicable, pursuant to art. 58, par. 2, lett. i), the administrative sanction provided for by art. 83, par. 5 of the Regulations, as also referred to by art. 166, paragraph 2, of the Code.

In this context, considering, in any case, that the conduct has exhausted its effects, also bearing in mind that the data controller immediately requested the reporting party to destroy the documentation received erroneously, ensuring confidentiality in this regard, and has implemented specific measures to avoid the repetition of the contested conduct, the

conditions for the adoption of prescriptive or inhibitory 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, par. 1, lett. f), 6 and 9 of the Regulations, caused by the conduct put in place by the Latina ASL, is subject to the application of a pecuniary administrative sanction pursuant to art. 83, par. 5, lett. a) of the Regulation and 166, paragraph 2, of the Code.

The Guarantor, pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, has the power to "inflict an administrative pecuniary sanction pursuant to Article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, depending on the circumstances of each single case "and, in this context," the College [of the Guarantor] adopts the injunction order, with which it also disposes with regard to the application of the ancillary administrative sanction of its publication, in whole or in excerpt, on the website of the Guarantor pursuant to Article 166, paragraph 7, of the Code "(Article 16, paragraph 1, of the Guarantor Regulation no. 1/2019).

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:

- the communication of personal data and, in particular, health data contained in the two documents concerned, in total, 5 people and had a single recipient not authorized to receive them (Article 83, paragraph 2, letter a) and g) of the Regulation);
- no intentional behavior on the part of the data controller emerges with respect to the matter, as it was a human error that occurred in the scanning phase of the documentation subsequently sent to the unauthorized third party (Article 83, paragraph 2, letter b ) of the Regulations);
- no measures concerning relevant violations have previously been adopted against the Healthcare Company itself (Article 83, paragraph 2, letter e) of the Regulation);
- the Company has always behaved collaboratively with the Authority (Article 83, paragraph 2, letter f) of the Regulation);
- the Company promptly took action by requesting the collaboration of the third party who came into possession of the data subject to the violation and by adopting technical and organizational measures aimed at preventing the repetition of the incident (Article 83, paragraph 2, letter c) and f ) of the Regulations);

- the Guarantor has become aware of the violation from the notification of violation by the Company and from the notification of the unauthorized third party (Article 83, paragraph 2, letter h) of the Regulations);

- the unlawful communication involved in the matter in question took place in the delicate context of the management and containment of the pandemic crisis in progress which subjected the health structures to considerable efforts (Article 83, paragraph 2, letter K) of the Regulation) .

Due to the aforementioned elements, assessed as a whole, it is believed to determine the amount of the administrative fine provided for in Article 83, par. 5, lett. a) of the Regulations, to the extent of € 10,000.00 (ten thousand) for the violation of Articles 5, 25, 32 and 37 of the same 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, due to the particular nature of the data processed.

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 Latina ASL with registered office in Latina, V.le Pierluigi Nervi - Tax Code: 01684950593 for the violation of articles 5, par. 1, lett. f), 6 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 ASL Latina, to pay the sum of € 10,000.00 (ten 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 Healthcare Company, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 10,000.00 (ten thousand) according to the methods indicated in the annex, within 30 days of

notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the 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, December 16, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Ghiglia

THE DEPUTY SECRETARY GENERAL

Philippi