[doc. web n. 9685332]

Injunction order against the Health Protection Agency of the Metropolitan City of Milan - May 13, 2021

Record of measures

n. 268 of May 13, 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, 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;

SPEAKER prof. Pasquale Station;

WHEREAS

1. The preliminary activity.

At the beginning of November 2020, the Office learned from press reports and some reports of the circumstance that, through

the "Milano COR" Portal, accessible at the address "https://milanocor.ats-milano.it/", it would have been It is possible to know if a citizen of the Milanese metropolitan area was, or had been, positive for Covid-19, simply by entering the tax code and mobile phone number on a page of the aforementioned Portal. In particular, if the subject - to whom the aforementioned data referred - was, or had been, positive, the Portal revealed that an account was already present for that subject (advising access via e-mail credentials and password); otherwise, he proposed registration to the service to the same, thus indirectly revealing the current or past positive state of Covid-19, as the aforementioned service was dedicated only to subjects falling into this category of users.

In this regard, on November 3, 2020, the Office carried out a remote assessment, the results of which were recorded in a service report in documents, from which what was represented in the press reports and in the aforementioned reports was verified and ascertained the deactivation of the service, in the manner described above, in the late morning of November 3, 2020.

In relation to the findings, information was requested from the Health Protection Agency (ATS) of the Metropolitan City of Milan (hereinafter the Agency) (note dated 3.11.2020, prot. reply with the note of 10 November 2020 (prot. no. 158410) also sending the impact assessment on data protection and the "information" model, drawn up pursuant to art. 13 and 14 of the Regulation, relating to the treatment in question. In the aforementioned note, the Agency has in particular represented that:

"In situations of extreme urgency and with the need to find information on the symptoms that were used to stratify the population, in order to allow the subjects at greater risk to be put on active surveillance, and as the number of uninvested cases increases, October 18 is a development based on information systems of the epidemiological investigation was released in which the positive subject was actively engaged, via an SMS, and invited to give information - which, at least in part, allow to guarantee the tracking functions useful for public surveillance purposes - on a portal prepared by the undersigned ATS. Therefore, an access system based on the tax code of the subject was immediately set up together with the telephone number, communicated by him, on which the SMS inviting him to join this new tracking method was received. At the same time, the study was launched for the activation of the third via sms key procedure aimed at improving access security. The development of the third key, in fact, requires programming, development times and resources that are not immediately available, so it is currently being tested ";

- “Once the positive subject had been identified by combining the two keys known to him (Tax Code and Telephone Number),

the user created his own profile by independently choosing a username and password associated with his profile. Entered passwords are stored in encrypted form. The user accesses a profile, in which he can enter information ";

- “in the first release of the Portal, there was only the indication of the date and place of the first buffer made by the user. Currently, in the version that will be released, this indication will no longer be reported ";

- "The participation of citizens was massive and about 30% of new cases had access to the Portal, also allowing the team that deals with epidemiological investigations to target interviews with minors, school cases and the most problems of cases that have arisen in some specific communities ";

- "In particular, the screen-shot of the" profile "page is shown which contains only the data entered by the user (username, social security number, date of swab and office but not the report" (screen-shot in documents) ;

- "In relation to the case under analysis, during the usual monitoring of the system and analysis of the application logs, a high number of accesses (about 47000) from the same user and IP address was detected: this event occurred verified approximately between 8.00 and 14:50 on November 2, 2020. Consequently, the technical analysis was started which led to the identification of the attacking IP and to proceed with the reporting to the Fastweb Network Provider at 18:45 on the 2nd November itself for the necessary measures. As per the attached email, Fastweb has taken steps to carry out the verifications of its respective competence ";

- “With respect to this event, ATS is finalizing the presentation of the complaint to the Public Prosecutor's Office. This massive access attempt came from the same IP address and related to the same user already registered on the portal. The information reported in the portal were only and exclusively referred to the subject himself and not to other subjects related to it, however, the specific subject had not filled out the questionnaire relating to symptoms, nor had he reported any information referring to the cohabitants. Furthermore, the data contained in the portal are only those self-entered by users. The analysis of the logs did not reveal any anomalies that required further investigation. Therefore, it was considered that it was not a Data Breach ";

- "The next day 3/11, ATS received news of a video published on Youtube which highlighted the presence of an application error relating to the response message to a partial registration, and therefore decided to temporarily suspend the registration function and control. This event led to the precautionary suspension of the portal starting from 3 November and at the same time starting the investigation for reporting to the competent authority ";

- “The number of interested parties involved in the treatment in question, distinguishing those already registered on the Portal

from those potentially recipients of the aforementioned services, is reported as follows: the cases involved are all cases that have arisen in the population since 10 October (43,185); the total registered cases included are 13,872; The number of interested parties who filled out the aforementioned "diary" was 7,944 ";

- "The number of cohabiting subjects who have been reported through the functions provided in the aforementioned Portal is nr. 13,596 and the identification of these subjects is part of the tracing best practices of any epidemiological investigation. With regard to cohabiting subjects, the interested parties could only enter the information listed below but not data / health reports: name, surname, tax code, mobile phone, date of birth and date of contact ";

- "the cases that were credited to the portal were about 30% of the cases arising per day, therefore 1000-1500 cases per day in the last week".

With specific reference to the measures taken in order to prevent episodes such as the one in question from recurring, the Agency also stated that the following measures were being adopted:

- "the portal will be restored with the activation of a third key which will be generated automatically, sent by SMS to the telephone number indicated by the person concerned at the time of making his / her swab. In particular, the system will work in this way: access to the portal and therefore also to the registration phase will be conditioned - in addition to the indication of the tax code and the mobile phone declared, also to the knowledge of a random code consisting of 6 digits (code alphanumeric) with a validity of about 5 minutes from receipt of the SMS (the exact determination of the validity time of the SMS will depend on the outcome of the texts for the correct timing). The random code will be transmitted exclusively to the mobile phone indicated by the person concerned at the time of taking the swab. This mechanism will be applied both to users already registered and to new interested parties, registered with reference to the swabs carried out by the SSR ";

- "The above solution also provides for a further check consisting in the insertion of a limited number of tax codes that can be consulted against a tax code, mobile phone, third valid key (with time validity) equal to a defined threshold, determined on the basis of an in-progress evaluation of the maximum number of family members who insist on a single telephone number (e.g., the parent's mobile phone and cohabiting children). Once the threshold is exceeded, the user is blocked and must send a report to a dedicated email box ";

- "Improvement of the LOG analysis mechanisms for the timely detection of any anomalies";

- "Improvement of the analysis process of IT security solutions and for the adoption of forms of protection and targeted

prevention mechanisms from external attacks";

- "Display of the information when registering on the Portal".

In relation to what emerged from the documentation, the Office notified the Agency, 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 December 2, 2020, prot. No. 45911).

In particular, the Office, in acknowledging the actions taken by the Agency to overcome the criticalities that emerged with reference to the methods of accessing the "Milano COR" Portal, considered that the provision of the services described, through the aforementioned Portal , occurred in a manner that does not comply with the principles of "integrity and confidentiality" and "data protection by default" (articles 5, par. 1, letter f), and 25, par. 2, of the Regulation), in the absence of technical and organizational measures suitable to guarantee a level of security adequate to the risk presented by the processing (Article 32 of the Regulation), in the absence of a prior assessment of the impact on data protection and in a non compliant with the principle of accountability (articles 5, paragraph 2, and 35 of the Regulation), as well as without having provided the data subjects with the information required by the regulations on the protection of personal data (articles 5, paragraph 1, letter a), and 13 of the Regulation).

With a note dated 31 December 2020, the Agency sent its defense briefs, in which what was already indicated in the aforementioned note of 10 November 2020 was reiterated and represented, in particular, that:

"Minors have never been allowed direct access to the portal with their own account and the collection of personal data of minors could only take place if reported as a contact by the positive user already registered within his / her exclusive profile";

"The data relating to the positivity to Covid19 could in the abstract be inferred only by those who were aware of the functioning of the portal (ATS and its representatives appropriately designated as subjects authorized for processing)";

"From what is known, no data breach has occurred, as the insertion of the tax code and telephone number on the portal home page only resulted in the opening of an information window without data or personal information, except the fact that, in the abstract, knowing the technical characteristics of the portal operation, with an articulated logical operation, it would have been possible to indirectly deduce the state of positivity, previous or past, based on the information message issued by the portal

after entering the correct data combination ",

"It should be noted that the insertion of an existing tax code gave rise to the message referred to above. This design feature was necessary considering that the epidemic involved entire families and problems were generated in accessing the service if the same user number provided at the time of the swab in the analysis laboratory was not entered in the portal. In any case, this is an articulated and elaborated operation, limited to the sole experience of the reporting user, since, otherwise, the security systems adopted by ATS and illustrated in the note of 10 November 2020 would have reported multiple or anomalous access attempts. coming from a single IP address ";

on the basis of the checks carried out, he believes that "the illegal access attempts were limited to the event of November 2, 2020 only";

"The above circumstances therefore allow us to believe that, even if we want to recognize a violation of the reference discipline in terms of the failure to adopt suitable measures from the design of the treatment, the extent of the same must be considered extremely slight, as the alleged violation: - was limited to a limited time frame (two weeks); did not result in the violation of personal data; did not cause damage to the parties concerned; it was immediately resolved with immediate action, and regardless of the communication of the Guarantor of November 3, 2020 ";

"ATS provided the information to interested parties required by art. 13 of the Regulations, directly in the section dedicated to the privacy policy of its website called up by the portal, which has remained unchanged since the entry into force of the Regulations (see attached information sub 5). The information contained therein is the general one used by ATS, which, as formulated, seems appropriate to also include the treatments carried out within the portal itself in the context of the health emergency caused by Covid19. (...) The circumstance that art. 9 of the Regulation in the paragraph does not seem sufficient to invalidate the correctness of the information in question, given that no provision burdens the owner from the obligation to indicate the references to the articles of the Regulation, it being sufficient that the contents of the information allow the interested party to understand the information required by the law, which in this case are provided ";

"In any case, it should be noted that art. 17-bis, paragraph 5, of the d.l. March 17, 2020, n. 18, provides that the public and private structures of the National Health Service "may omit the information referred to in Article 13 of the same regulation or provide simplified information, subject to oral communication to those affected by the limitation". The circumstance that the legislator has exempted health facilities such as ATS from the obligation to provide the information, undoubtedly allows us to

consider the charge made to ATS exceeded, which, by doing more than was required by the law, provided in writing through its website the communication relating to the fact that the treatment was carried out for the purposes of territorial health and social health planning integrated with the social one, as well as for purposes of hygiene and public health. The lack of oral communication of the limitation, however impossible in the present case in which the data processing takes place online, despite being provided for by the law, does not receive any sanction from the legislator, constituting a mere indication of a programmatic nature. Nor can it be considered that the oral communication of the limitation constitutes the prerequisite for making use of the exemption from the obligation to provide information, in violation of the principle of mandatory and specific administrative sanctions. It seems unreasonable to the writer to believe that an exceptional rule issued during an unprecedented state of emergency charges the healthcare facility that is the data controller to inform the data subject that no information will be provided, under penalty of deeming the derogated discipline applicable with relevant penalties. " (...) A constitutionally oriented interpretation of the aforementioned art. 17-bis, paragraph 5, can only lead to consider that the exemption from the obligation to provide the information required by the aforementioned provision is applicable to the case in question, also considering the Agency's conduct perfectly legitimate and indeed commendable, regardless of the failure oral reference of the limitation referred to in the aforementioned art. 17-bis (...). In any case, it must be noted that, after the first communication from the Guarantor on 3 November 2020, ATS acknowledged the suggestion provided, preparing a separate information document intended to exclusively regulate the processing underlying the use of the portal ";

"Excluding then the existence of the fraud, given that in the documents there are no elements that could lead to believe that the programming of the portal was intentionally deficient in relation to the disputed profiles, it is necessary to understand whether the alleged - and contested - violation in question can be attributed to the Agency by way of fault ";

"From this point of view, this defense believes that, although the alleged violation originates from a possible gap in the programming of the portal, the context of absolute exceptionality and emergency1 in which ATS was operating excludes the existence of the element of fault required by the rules of reference to for the purposes of punishing the conduct and therefore the imposition of any sanctions ";

considers "the conduct of ATS in the specific context is not punishable, given that, even if one wishes to recognize the integration of a violation, the responsibility of the data controller appears non-existent due to force majeure";

"The main measure taken to mitigate the effects of the violation for the data subjects was to suspend the portal on November

3, 2020, restoring its operation only after the integration of the security and organizational measures";

"As illustrated in the note sent on November 10, 2020, as soon as the first communication from this Authority was received, ATS created a" third key "for authentication to access the portal, integrating the same with specific information pursuant to art. 13 of the Regulations ";

with regard to "the identified violation consisting in the failure to adopt the impact assessment in the first period of operation of the portal previously indicated (from 18 October 2020 to 3 November 2020)", "the activation of the portal was occasioned by the urgent need to cope with the sudden management of Covid patients19. The peculiar emergency context required immediate activation, not compatible with the adoption, albeit prudential, of an impact assessment. In any case, the requirements that require the carrying out of the aforementioned assessment appear to be lacking. The portal was in fact intended to contain only the registration of information revealing the state of positivity, previous or present, to Covid19, without containing reports, health data or other information that could "present a high risk" for the interested party (art. 35 of the Regulation). The concept of high risk is not necessarily identified with the particular nature of the data pursuant to art. 9 of the Regulations. Paragraph 3 of the aforementioned art. 35 indeed exemplifies the hypothesis in which the processing of particular categories of data is carried out on a large scale, which does not seem to be possible in the present case. First of all, in fact, it must be considered that the portal was activated in a period (starting from 18 October 2020), in which it was not possible to predict the number of subjects who would have used the portal itself (number which, as illustrated , turned out to be about three quarters lower than those actually infected). Secondly, the concept of large scale should be related to the number of inhabitants of the metropolitan area of Milan, which has about 3,500,000 individuals. A few thousand users, randomly located in such a populous Region, should not integrate the large-scale requirement required by the aforementioned provision. [...] In any case, ATS also carried out the impact assessment of November 9, 2020 as soon as requested by this Authority ".

2. Outcome of the preliminary investigation.

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

personal data must be "processed lawfully, correctly and transparently" (principle of "lawfulness, correctness and transparency") and "in such a way as to guarantee adequate security (...), including protection, through appropriate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage

(principle of "integrity and confidentiality") "(art. 5, par. 1, lett. a) and f), of the Regulation);

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 then provides that the data controller implements "adequate technical and organizational measures to ensure a level of security appropriate to the risk", taking into account, among other things, "the nature, object, context and purpose of the processing, as well as the risk of varying probability and gravity for the rights and freedoms of individuals "and that" in assessing the adequate level of security, special account is taken of the risks presented by the processing that derive in particular from the destruction , from the loss, modification, unauthorized disclosure or access, accidentally or illegally, to personal data transmitted, stored or otherwise processed "(Article 32 of the Regulation);

the data controller must also comply with the principle of "data protection by default", according to which it must "put in place appropriate technical and organizational measures to ensure that, by default, only the personal data necessary for each specific purpose of the processing "with reference to" the amount of personal data collected, the scope of the processing, the retention period and accessibility ", ensuring, in particular," that, by default, they are not made personal data accessible to an indefinite number of natural persons without the intervention of the natural person "(art. 25, par. 2, of the Regulation).

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 provisions on the protection of personal data relating to the security of processing (Article 32 of the Regulation) and to the assessment of the impact on data protection (Article 35 of the

Regulation);

on the basis of what was ascertained, the measures initially adopted allowed anyone to know if a citizen of the Milanese metropolitan area was, or had been, positive for Covid-19, simply by entering his tax code and the relative mobile phone number in a page of the aforementioned Portal. If the subject - to whom the aforementioned data referred - were (or had been) positive, in fact the Portal revealed that an account was already present for this subject (advising access via email credentials and password), or proposed to the same registering for the service. In the event that the subject was not (or had been) positive for Covid-19, it was possible to proceed with the creation of the account. Given the service offered through the aforementioned Portal, it was therefore possible to trace a subject's current or past Covid-19 positive state (https://www.ats-milano.it/portale/In-primopiano/novusact/viewarticle/ articleid / 3445);

the methods of access to the aforementioned service described above, chosen by the Agency to identify users in the registration phase until 3 November 2020, were not suitable for averting the risk that unauthorized subjects could easily know the positive status, also in the past, of some people, simply by entering their tax code and mobile phone number in the aforementioned Portal;

the monitoring systems used by the Agency made it possible to detect unauthorized access only afterwards, thus being inadequate to prevent the timely verification of the positive state (current or previous) of a subject simply by entering the tax code and telephone number of the same ;

the failure to adopt adequate measures to ensure that, by default, personal data of the data subjects who tested positive for Covid 19 were not made accessible to an indefinite number of people, is contrary to the principle of "data protection by default "(Art. 25, par. 2, of the Regulations);

differently from what is believed, the case in question is among those for which the owner is required to carry out, "before proceeding with the treatment, an assessment of the impact of the treatments envisaged on the protection of personal data" (Article 35 of the Regulation) . This is because, for the treatment in question, two of the criteria indicated by the European Data Protection Committee are certainly used to identify the cases in which a treatment must be subject to an impact assessment. In particular, reference is made to the following criteria: processing of "sensitive or highly personal data" and "data relating to vulnerable interested parties" which include patients (see Guidelines on impact assessment on data protection and determination of the possibility that the processing "may present a high risk" for the purposes of Regulation (EU) 2016/679

adopted on 4 April 2017, as amended and last adopted on 4 October 2017, and endorsed by the European Committee for data protection on 25 May 2018 - WP 248 rev.01, III, lett. B, points 4 and 7). It is then believed that, with reference to the present case, the criterion relating to "large-scale data processing" may be satisfied, even if only potentially, considering that, according to the Agency's declaration, joining the service is it was “massive” and involved thousands of interested parties in just two weeks (see the aforementioned Guidelines, III, lett. B, point 5);

according to the provisions of the Regulation, the aforementioned impact assessment must be carried out before proceeding with the processing of personal data and must contain precisely those measures to deal with the risks and to guarantee the protection of personal data, the adoption of which would certainly have avoided the event ;

in this regard, the Agency has instead sent an impact assessment which appears to have been drawn up only on 9 November 2020, or after the activation of the aforementioned service on the “Milano COR” Portal and therefore in breach of the accountability principle (art. 5, par. 2, and 35 of the Regulation) and the same is, however, lacking in the examination of the specific risks of unauthorized access described above and referable to the case in question;

the facts in question are not considered to have occurred due to force majeure, or are attributable to extraordinary or unforeseeable events such as to exclude liability, rather than they are due to a (culpable) failure to evaluate, expressly required by the regulations in protection of personal data, the risks of processing with the consequent failure to adopt measures to reduce the aforementioned risks. These measures were put in place by the Agency only subsequently "as soon as the first communication from this Authority is received" by inserting a "third key" for access to the portal. The speed and simplicity with which the Agency solved the problem highlighted by the Authority show that the facts in question could have been avoided by the owner and therefore are not attributable to force majeure;

with specific reference to the information to be made to interested parties pursuant to art. 13 of the Regulation, the legislator, in the emergency context in progress, has provided that the subjects operating in the aforementioned context, including the public and private structures of the National Health Service, may "fail to provide the information" referred to in the aforementioned article 13 "or provide a simplified information, subject to oral communication to the parties concerned by the limitation" (Article 17-bis, paragraph 5, Legislative Decree 17/03/2020, n. 18). Given this, it cannot be considered that the aforementioned provision can be considered an absolute exemption from the obligation to provide the information referred to in Articles 13 and 14 of the Regulations, especially in cases, such as the present one, where the implementation of this

requirement does not constitute a hindrance and does not entail a delay in the provision of a service, albeit in the context of an emergency. In this regard, it should be noted that, for all the treatments authorized by the Authority in the emergency context, it has been provided that the aforementioned information is provided to the interested party even if in a simplified manner (see, ex multis, measures adopted with reference to the processing of data carried out in the context of the Covid 19 alert system - Immunity App - provisions of 1.6.2020 and 25.2.2021). With specific reference to the case in point, it should be noted that no particular complexity or need for extraordinary actions and resources is evident in the publication of the information indicated in the Regulations on the aforementioned Portal;

in noting that the Agency, as indicated in the documents, has not communicated to the interested parties its intention to make use of the possibility offered by the aforementioned art. 17-bis of the D.L. 17/03/2020, n. 18, regarding the information to be provided to the interested party, not even at the time of the swab execution, it is noted that the model called "Information on the processing of personal data of ATS Milano in the Milano Cor portal" drawn up by the Agency pursuant to Articles . 13 and 14 of the Regulation, in use until December 2020, does not comply with the requirements of the regulations on the protection of personal data. In particular, contrary to what the Agency maintains, the data controller must indicate, among the information to be provided to the interested party, also "the legal basis of the processing" (Article 13, paragraph 1, letter c), of the Regulation). Furthermore, the text of the information model in the documents did not provide precise indications regarding the specific processing carried out and the purposes pursued (articles 9 and 13 of the Regulation and articles 2-sexies, 77 et seq. Of the Code).

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 ATS of the Metropolitan City of Milan, in the terms set out in the motivation, is noted, in violation of Articles 5, paragraph 1, lett. a) and f), and par. 2, 13, 25, 32

and 35 of the Regulation.

In this context, considering, in any case, that the conduct has exhausted its effects, given that the Agency has changed the methods of accessing the aforementioned Portal and that a new model has been drawn up through which to provide information to interested parties referred to in art. 13 of the Regulation before the provision of personal data by the same, which indicates the purposes pursued and the legal bases of the processing, the conditions for the adoption of the corrective measures referred to in art. 58, par. 2, of the Regulation.

However, it should be noted that the new disclosure model adopted by the Agency present on the Milan COR Portal (https://milanocor.ats-milano.it/freedownload/privacy) does not clearly indicate the person responsible for the processing and the scope of any transfer of data to third countries.

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, par. 1, lett. a) and f), and par. 2, 13, 25, 32 and 35 of the Regulations, caused by the conduct put in place by the ATS of the Metropolitan City 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 seriousness of the violation committed is high and the damage suffered by the interested parties is considered not low but medium (Article 83, paragraph 2, letter a), of the Regulations);

the Authority became aware of the event following press reports and reports (Article 83, paragraph 2, letter h), of the

Regulations);

the processing carried out by the Agency concerns data suitable for detecting information on the health of a significant number of data subjects (Article 83, paragraph 2, letters a) and g), of the Regulation);

the Agency immediately demonstrated a high degree of cooperation, endeavoring 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, paragraph 2, letters c), d) and f), of the Regulation);

before the Agency introduced new methods of access to the aforementioned Portal, the previous methods, highlighted above, were used only for a limited period of time (two weeks) (Article 83, paragraph 2, letter a) and c) , 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 80,000 (eighty thousand) for the violation of 5, par. 1, lett. a) and f), and par. 2, 13, 25, 32 and 35 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 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 Health Protection Agency of the Metropolitan City of Milan for the violation of Articles 5, par. 1, lett. a) and f), and par. 2, 13, 25, 32 and 35 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 Health Protection Agency of the Metropolitan City of Milan, tax code 09320520969, in the person of the pro-tempore legal representative, to pay the sum of 80,000 (eighty thousand) euros as a fine 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 Agency, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 80,000 (eighty 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;

pursuant to art. 157 of the Code to provide, within 30 days from the date of communication of this provision, clarifications regarding the designated person responsible for the processing and the scope of any data transfer to third countries indicated in the information model present on the Milano COR Portal (https: //milanocor.ats-milano.it/freedownload/privacy);

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, May 13, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Stanzione

THE SECRETARY GENERAL

Mattei