[doc. web n. 9744496]

Injunction order against the Marche Regional Health Authority - 13 January 2022

Record of measures

n. 9 of 13 January 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 the lawyer Guido Scorza, members, and the Cons. Fabio Mattei, general secretary;

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

GIVEN the legislative decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national system to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of individuals with regard to to the processing of personal data, as well as to the free circulation of such data and which repeals Directive 95/46 / EC (hereinafter the "Code");

GIVEN the Legislative Decree 10 August 2018, n. 101 on "Provisions for the adaptation of national legislation to the provisions of 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 repealing Directive 95/46 / EC ";

GIVEN the Regulation n. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved by resolution no. 98 of 4/4/2019, published in the Official Gazette n. 106 of 8/5/2019 and in www.gpdp.it, doc. web n. 9107633 (hereinafter "Regulation of the Guarantor no. 1/2019");

GIVEN the documentation in the deeds;

GIVEN the observations made by the Secretary General pursuant to art. 15 of the Guarantor Regulation n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, Doc. web n. 1098801;

Speaker Dr. Agostino Ghiglia;

WHEREAS

1. The preliminary activity

1.1. Press news

A press release dated January 6, 2021, reported in "Il manifesto", available at: https://ilmanifesto.it/marche-il-buco-dello-screening-dati-accessibili-a-chiunque, gave evidence of a vulnerability in the Covid-19 screening data acquisition and management system, in relation to the possibility of third party access to some personal data (name, surname, mobile number and, in one case, the result of the swab carried out as part of a Covid-19 screening program) of the assistants of the Marche Region Health Authority (hereinafter the "Company"). In particular, through the use of the App called "Smart4You", it was possible to read the QR Code on the slip issued to anyone who had undergone screening for Covid-19, in order to consult "their medical dossier with medical records , the various hospital bookings made and the relative outcomes ". According to what is reported in the aforementioned press release, this code "was not (was) processed randomly, but follows a simple progressive criterion: each number corresponds to a user and it is enough to change a digit to access someone else's profile".

Following the aforementioned press report, the Office requested information from the Marche Region which had, in this regard, given notice of the aforementioned service in a press release (https://www.regione.marche.it/In-Primo-Piano/ComunicatiStampa // id / 29699 / p / 1 / OPERAZIONE-MARCHE-SICURE-FROM - TO - JANUARY-SCREENING-FOR-CITIZENS-OF-SAN-BENEDETTO-DEL-TRONTO) (see note of XX , prot. no. XX).

In response to the Office's request for information, the Marche Region, with a note of the XXth, stated that "the Regional Council does not have the ownership of the treatment, nor any other responsibility in terms of protection of personal data connected to the reported event ”And submitted a report by the Company's Data Protection Officer, in which it was represented that the latter had notified the Authority of the violation, pursuant to art. 33 of the Regulations and to submit a complaint to the Postal Police in the event of unauthorized access to the regional computer system.

1.2. Notification of Infringement

The aforementioned notification, made on XX, was, following further investigations and investigations, subsequently integrated on XX.

As part of the aforementioned notifications, it was stated that "" in the article the screening activities are confused with the

information related to the electronic health dossier in use at the Vast Area 5 of ASUR Marche. In reality, in the databases, the screening and dossier requests are completely separate, although both can be reached from the website https://www.cureprimarie.it, accessible in completely different ways from an authorization and authentication point of view "(v. notification of the XX, section C point 5, which refers to the attachment "Documentation of data breach integration no. XX of the XX", paragraph "Summary for the evaluator"; in this sense also the notification of XX, section D point 1).

According to what is indicated in the aforementioned documents, the vulnerability - present from mid-December to 6 January 2021 - would have concerned the screening management platform, (https://www.cureprimarie.it) limited to the "Screening COVID-19 San Benedetto" service, and the "Smart4You" app connected to the same screening in relation to the quick reading function of the result of your swab via a sequentially generated QR-code that was delivered only to the participants in the Covid-19 screening activities in the initial stages of acceptance and that directly associates participant-buffer outcome (see note of XX, section D point 1).

More specifically, with regard to the "Smart4You" app, the Company specified that: the same application required registration by the client by entering an e-mail address, a mobile phone number and the OTP code, sent to the mobile number indicated in the initial booking phase; there were 35 people affected by the vulnerability (sequential coding for identifying the result of the buffer) (see note of XX, section C, point 11 and attachment "Data breach integration documentation no. XX of XX", par . "Summary for the evaluator"); the violation is “limited to personal data and, where present, to the subject's mobile phone number. In no case are accesses to the results of the swab, unless a single attributable to the person who forced the system "; "A former employee of the supplier of the Electronic Health Dossier application (NBS Srl), installed in the Vasta Area no. 5 of ASUR Marche, made 35 unauthorized accesses "(see note of XX, section C, point 11 and attachment" Data breach integration documentation no. XX of XX "par." Summary for the evaluator ").

With specific reference to the "Screening COVID-19 San Benedetto" service offered by the screening campaign management platform (https://www.cureprimarie.it), the Company declared that the vulnerability (decoding of the tax code) was present in the first version of the tampon reservation service, since “at first, the application designers had provided for an unusual reservation method which, following the insertion of the tax code, allowed the automatic decoding of the corresponding name. Only at a very early stage of the screening was the possible mobile phone number also shown but only if previously registered "and that although" the risks of automatic decoding of the population residing in the province of Ascoli Piceno, in a brutal force

style, are evident ... there is no evidence of anomalous behavior on the part of users "(see annex note of XX" Documentation of data breach integration no. XX of XX ", paragraph" Summary for the evaluator ").

The Company also specified that "the vulnerabilities would certainly have been avoidable in a moment of normal activity, according to the validation procedures in place. Unfortunately, the emergency due to the pandemic has resulted in an urgent implementation irreconcilable with the time required for an adequate design in terms of safety "(see attachment to the note of the XX" Documentation of data breach integration n. XX of the XX "par." Summary for the evaluator ").

The measures indicated by the Company, aimed at guaranteeing the security of the processing existing at the time of the violation of the personal data subject to notification, are:,,:: "https protocol, log of accesses and activities carried out, systems monitoring, monitoring of user behavior, registration and authorization procedure through identification of subjects at the company URP, credentials recovery only through pre-registered tools and devices, implementation of the AAA Protocol, implementation of the Separation of Duties (SoD) paradigm with management of authorization profiles, daily backup of data and logs, penetration tests carried out with positive results (no serious or medium elements) ", for the www.cureprimarie.it platform,": "https protocol, log of accesses and activities carried out, systems monitoring, use of QR □ code for pseudonymisation of the results of the swabs, registration by sending SMS d part of the activation code, implementation of the AAA Protocol ", for the" Smart4You app (see attached to the note of the XX “Documentation of data breach integration n. XX of the XX ", par. 4).

With regard to the measures adopted to remedy the violation of personal data and to mitigate the possible negative effects on the interested parties, the Company has stated that, following the facts covered by this provision, the NSB supplier has changed the generation of the QR-code with a more complex hash-type coding, consisting of a first part of the fiscal code combined with a random sequence, and has requested the immediate implementation of the following security measures: "elimination of the fiscal code decoding functionality with the name of the regional clients, reduction of the subjects verifiable at the regional registry to residents of the territories subjected to screening only, verification of the consistency between the mobile number with the Smart4you app and the subject questioned, also including the possibility of blocking or at least alerting, elimination of the SMS functionality with the name and results reported, banning deg the IP addresses from which repeated requests, multiple registrations or requests with incorrect encodings or accounts come "(v. attached to the note of the XX “Documentation of data breach integration n. XX of the XX ", par. "Summary for the evaluator" and sect. F, point 1).

With regard to the measures adopted to prevent similar violations in the future, the Company declared that it had defined a more rigorous procedure for the acquisition of corporate web platforms, software applications, as well as mobile Apps, also through a "sort of product qualification / service starting from the basic principles of the regulation such as integrity and confidentiality of information, in addition to privacy by default and by design, combined with security by design "which includes a" vulnerability assessment, specific penetration tests in order to first highlight any flaws in the system, the use of AgID qualified platforms subjected to OWASP type penetration tests "(see attachment to the note of the XX" Documentation of data breach integration n. XX of the XX ", section F, point 2).

Finally, the Company declared that the violation was an opportunity to draw "from the event a series of elements that will be actively taken into consideration in future actions and behaviors by third parties" and that "many of the vulnerabilities were found and resolved independently before reporting the violation by the journalist. Other vulnerabilities were resolved at the request of the DPO "(see attachment to the note of the XX" Documentation of data breach integration no. XX of the XX ", paragraph" Lesson learned ").

In relation to what emerged from the documentation and the notification of violation, the Office, with a note of the XX (prot. No. XX), notified the 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 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).

In particular, the Office, in the aforementioned deed, identified the details of a violation of the principles of integrity and confidentiality, of the obligations of the data controller in terms of data security and impact assessment on data protection (art. 5, par.1, lett.f), 32 and 35 of the Regulation) as well as art. 75 of the Code which is without prejudice to the specific sector provisions contained in the d.P.C.M. 8 August 2013, regarding online reporting; this, in consideration of the methods of generation of the sequential identification of the swabs carried out by the interested parties and of the decoding of the tax code of a client in the context of the "Screening COVID-19 San Benedetto" service, of the use of SMS to communicate the outcome swabs to data subjects, as well as the failure to assess the impact on data protection.

With a note from the twentieth century, the Company sent its defense briefs in which, in particular, after describing the company organization, it highlighted that:

- the "booking activity, (...), at that precise historical moment had to fulfill at least two requirements: to manage the influx of people in an orderly and safe way so as not to create gatherings, as well as to guarantee the correct management of all resources , starting from the sanitary staff up to the material delivery of the rapid tests ";

- "the fact that a subject, former supplier of ASUR Marche for the health Dossier, has proposed a full-service capable of solving the above-mentioned problems, both on the common side for bookings and on the health company side for the complete operation on tampons, is a low cost and immediate solution appeared to the Director of Area Vasta 5; to consider, always and in any case, the expected timing of implementation of the particularly stringent screening and, at least apparent, compliance with the obligations and requirements in consideration of the pre-existing infrastructure ";

- "the timing available for the development of any integration with national systems was incompatible with a validated solution, since the urgency of the immediate activation of screening was driven not by mere statistical needs, but by the real need to identify the infected subjects , as far as possible before the Christmas holidays, a moment of family and extra-family conviviality; therefore, a period subject to greater risk of outbreaks ";

- "the adoption of a platform already active for some time, consisting of a web part and a mobile app component, for which not only the obligations related to the regulations on the protection of personal data had already been carried out, but also repeated tests of penetration, as a requisite in other supplies, were elements that certainly corroborated, in a positive way, the decisions of the Director of Area Vasta n. 5 with regard to the profile of the security guaranteed by the supplier, to the extent that consultation, even informal, of the DPO is not necessary ";

- "Since these are processing activities experienced as a simple integration between booking and reporting, which are pre-existing, and not as a new treatment of health data, it was not deemed necessary, at the time, to proceed with the obligations provided for in art. 35 GDPR or, more directly, request an opinion from the DPO office ";

- “in this case a series of unfortunate events, in an anxious context for the health situation and, moreover, with a very short timeframe, led to a series of comfortable and functional choices perceived by the patients themselves. However, the occasion is also useful to highlight how the ASUR Marche and the DPO, having just become aware of the choices made by the Director of the Vasta Area n. 5 and, above all, by the supplier, immediately took action by providing prescriptions and subjecting the same to a specific audit ";

- "The" Safe Marches "screening operation for the Vast Area no. 5 in the 6 days of activity (18/19/20/21/22 and 23 December)

received participation from 11,572 people, with a percentage of the target population of 24.6%, while at the level of total numbers of tests in the region, as already indicated, as of 31 December 2020 over 70,800 tests had been carried out. These numbers are extremely relevant in order to correctly frame the incident, considering that the violation that was the subject of the data breach, as already documented by the supplier, concerned only 2 subjects, both negative to the virus, who deliberately "forced" the system ";

- "the information on the negativity of the tampon also has a certain value, since it is undeniable that from the point of view of the perceived risk, having as a reference the freedom and dignity of the interested parties, as well as the possibility of any discrimination, especially in a emergency context and general screening linked to the historical moment, does not seem to be information capable of producing evident damage ";

- "it remains understood that, even if with significance and therefore extremely limited validity (maximum of 48 hours, for example, for the Green Pass), the result of a swab is to be considered to all intents and purposes a report, so correctly the Authority cites the Legislative Decree 137/2020 for the correct management of the document by coding through the so-called NRFE. Unfortunately, in the specific historical moment characterized by the rage of the COVID 19 pandemic, the systems in use were not yet compatible with these methods. Moreover, the digital divide of the large part of the population, even of the target type, does not now have and did not possess at the time neither SPID credentials, nor had any idea of what the FSE was, nor was it aware of other systems for consulting different reports. compared to what has already been done and known for other services ";

- "The perception of security, induced, in general, by the use of instant messaging tools was paradoxically appreciated by all those who participated in the screening. Except as reported in the article of the Manifesto, the healthcare company has not received any complaints from the patients for the chosen communication methods, despite all the known limitations of the SMS tool ";

- “the possibility of knowing the results of other screening participants through QR-code sequencing appears potentially impacting, but with lower implications. This is because having only one QR-code available, it is difficult to think of a simple, easily decipherable sequence, precisely as a function of the unforgivable mistake. Another issue is the production, printing, re-registration of the app to get to the reading of the other QR codes, of the subjects present at the screening sessions; however, the operation is not within everyone's reach and operationally requires a lot of time. Beyond the subjects actually

consulted, with a 0.2% probability of finding positive for COVID-19, this method, then corrected, appeared yet another lightness on the part of the supplier, who trusted in the difficulty of decoding a complex and visual code, such as the one used. Also in this case and preliminarily in the coding phase, the implementation of a simple hash function would have solved the problem without particular difficulties ";

- “with regards to an overall view of the data breach, it is necessary to refer to the probability function of the risk, in order to understand the real extent of the events. Starting from the basic definition of risk, i.e. considering the product between probability and impact, it is good to highlight a substantial difference between the impact actually suffered by the subjects, compared to the different potential impact considering the possible scenarios that can be assessed on various levels of severity. In fact, the actual violation highlighted in the post-event analysis phase did not really impact a significant number of subjects (...) (2 out of over 11,000 in the Vast Area, 2 out of over 70,000 in the Region). On the other hand, the point of view with respect to the exposure to the risk of exfiltration of the data on the outcome of the swab is totally different for all the participants in the screening, without prejudice to the duration of validity of the swab, which at the time was to be considered as a valid outcome. only for that moment, as no green certification is active. Another aspect to consider is that, net of an intentional action to change the sequential code, once the violation has been carried out, telephone numbers and names could have been displayed, starting from the tax code in the period of exposure. However, this exposure had a rather short duration, of a few days, corrected independently by the supplier itself as the ASUR intervened immediately, at the time of reporting ".

The same Company, in relation to the elements identified by art. 83, par. 2, of the Regulations, stated, among other things, that "with regard to the seriousness it is to be considered that the interested parties of reference are n. 2 out of over 70,000 swabs in that period. It should be noted that both interested parties are those who have voluntarily forced the system by accessing each other's data. There are no other violations against other interested parties, especially those who tested positive for the covid "; “As soon as the vulnerability of the system in use became known, the Management immediately took action to suspend it, providing prescriptions to the supplier and subjecting the same to a specific audit”.

2. Outcome of the preliminary investigation

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

- the information subject of the notification constitutes personal data relating to health, which deserve greater protection since

the context of their processing could create significant risks for fundamental rights and freedoms (Cons. No. 51 of the Regulation);

- the rules on the protection of personal data establish that the same data must be "processed in a manner that guarantees adequate security (...), including protection, by means of adequate technical and organizational measures, from unauthorized or illegal processing and from accidental loss, destruction or damage ("integrity and confidentiality") "(Article 5, paragraph 1, letter f) of the Regulations);

- regarding the security of processing, art. 32 of the Regulation, establishes that "taking into account the state of the art and the costs of implementation, as well as the nature, object, context and purpose of the processing, as well as the risk of varying probability and severity for the rights and freedom of natural persons, the data controller and the data processor implement adequate technical and organizational measures to ensure a level of security appropriate to the risk [...] "(par. 1) and that" in assessing the adequate level of security is especially taken into account the risks presented by the processing that derive in particular from the destruction, loss, modification, unauthorized disclosure or access, accidentally or illegally, to personal data transmitted, stored or otherwise processed " (par. 2). In any case, the data controller is required to adopt procedures "to test, verify and regularly evaluate the effectiveness of technical and organizational measures in order to guarantee the security of the treatment" (Article 32, paragraph 1, letter d));

- in relation to the possibility of consulting - electronically - the reports, including those relating to the outcome of the swabs for Covid-19, the Authority has adopted the "Guidelines on the subject of online reports "(Provision of 19 November 2009, available on www.gpdp.it web doc. No. 1679033, deemed compatible with the aforementioned Regulation and with the provisions of Legislative Decree no. 101/2018; see art. 22, paragraph 4, of the aforementioned legislative decree no. 101/2018), in which it is provided that "in the case of use of the SMS alert service of the availability to consult the reports through the methods described above, the message sent must be only given notice of the availability of the report and not of the detail of the type of investigations carried out, of their outcome or of the authentication credentials assigned to the interested party "(see point 2 of the aforementioned provision). Subsequently, the decree of the President of the Council of Ministers of 8 August 2013 was adopted concerning the methods of delivery, by health companies, of medical reports via the web, certified e-mail and other digital methods, as well as for making the payment online. line of services provided, on which the Guarantor has expressed a favorable opinion. In particular, it was envisaged that "the healthcare company may make

additional additional services available to the interested party to favor or facilitate the use of online reporting services, or to improve, in general, the quality of the services offered by the same" between which "Notification services" that "allow the interested party to request to be notified of the digital report being made available by sending a short message service (sms) to the mobile phone number or by sending a message to the e-mail address indicated in the act of accession to the online reporting services "(see Attachment A, point 2.a) to the aforementioned decree);

- the aforementioned decree falls within the specific sector provisions without prejudice to art. 75 of the Code, which summarizes the conditions for the processing of personal data for the purpose of protecting health in the health sector;

- the so-called decree "Ristori", in order to implement the diagnostic system of cases of positivity to the SARS-CoV-2 virus through the execution of swabs, has provided for a reporting system of the same that was defined by decree of the Ministry of Economy and finances, in agreement with the Ministry of Health, subject to the opinion of the Guarantor for the protection of personal data (Article 19, Legislative Decree No. 137/2020). Given the aforementioned sector regulations, this decree, based on the observations made by the Guarantor, also provided that only the unique electronic report number (NRFE) of the swab could be communicated via SMS and not its outcome (see decree of Ministry of Economy and Finance of 3.11.2020 and the opinion issued - on the same date - by the Guarantor on the aforementioned decree scheme, web doc n. 9563445). Similar provisions have been introduced in the context of the national telephone response service for health surveillance (see Opinion on the order scheme of the extraordinary Commissioner for the implementation and coordination of the measures necessary for the containment and contrast of the epidemiological emergency COVID -19 of December 17, 2020, web doc no. 9516719);

- in relation to the sequential identification of the swabs carried out by the interested parties and the decoding of the tax code of a client in the context of the "Screening COVID-19 San Benedetto" service, in during the investigation it was found that:

• the QR-code delivered to the participants in the Covid-19 screening activities was generated through a sequential coding, with a direct participant-result swab association. Therefore, by generating QR-code in sequence with respect to a first code in the possession of a third party, it was possible to view personal data and, where present, also the mobile number of the subject involved in the screening, as well as the results of the swab (ascertained only by of the person who forced the system);

• the "Screening COVID-19 San Benedetto" service offered through the screening management platform (https://www.cureprimarie.it) allowed the decoding of the tax code: following the entry of the tax code of a client, his name and surname and, at first, also the mobile number that may be present in the database. This method of verifying the data entered

by the clients, provided for by the supplier (data controller), was considered excessive and the General Management proceeded with note prot. XX of the XX to communicate to the Direction of Area Vasta n. 5, referent for the supply and screening activities for the province of Ascoli Piceno, the need to eliminate excess functionality and the implementation of appropriate technical measures;

• the failure to adopt a more complex coding, such as the one adopted after the twentieth century, as well as the possibility of decoding the tax code by third parties also through automatic methods (eg. Bot), are in contrast with the provisions of which to art. 5, par. 1, lett. f), and art. 32 of the Regulation;

- with reference to the use of SMS to communicate the outcome of the swabs, it was found that the communication of the outcome of the swabs, both negative and positive, was carried out by means of a short message service (sms). This choice - subsequently modified, in order to use the communication service via SMS only to report the availability of an outcome / report (platform or app) or for the management of reservations excluding the information related to each health service - was motivated by the simplicity and immediacy of the technological solution and also from the emergency situation, in order to avoid gatherings as the subjects subjected to screening were invited to remain in their cars until the message arrived on the telephone and in the case of a positive swab, the subject was subjected to further investigations; therefore, in light of the regulatory framework described above, at the time of notification, the sending of health-related data by SMS did not comply with the Guidelines on the subject of online reports of November 19, 2009 (Official Gazette No. 288 of 11 December 2009), to the provisions of the aforementioned d.P.C.M. of 8 August 2013 and the aforementioned provisions;

- the treatment in question is one of 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: "sensitive or highly personal data", "data relating to vulnerable data subjects" which include patients (see guidelines on impact assessment on data protection and determination of the possibility that the treatment "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 - WP 248 rev.01, III, lett . B, points 4 and 7). With reference to the present case, the following criteria can also be potentially met: "large-scale data processing" and "innovative use or application of new technological or organizational

solutions" (see the aforementioned Guidelines, III, lett. . B, points 5 and 8);

- the same data processing was carried out as part of the actions promoted to combat the epidemic from Covid -19. In this regard, it is noted that, since the declaration of the state of emergency resolved by the Council of Ministers on January 31, 2020, many urgent regulatory acts have been adopted, which also contain provisions relating to the processing of personal data carried out in the context of interventions relating to the aforementioned health emergency. That said, it should be noted that the emergency 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 the European 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. It is also noted that 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 impact assessment on data protection (Articles 35 et seq. Of the Regulation); in this regard, it should be noted that the impact assessment was not carried out in contrast with the provisions of the aforementioned art. 35 of the Regulation.

3. Conclusions

In light of the aforementioned assessments, taking into account the statements made by the data controller during the investigation and considering that, unless the fact constitutes a more serious crime, anyone, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces false deeds or documents, is liable pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor", the elements provided by the data controller in the aforementioned defensive briefs, which acknowledge what was contested in the act of initiating the procedure referred to in art. 166, paragraph 5, of the Code, are not suitable for accepting the archiving requests formulated in the defense briefs, even if they are worthy of consideration, and do not allow to fully overcome the findings notified by the Office with the aforementioned act of initiating the procedure.

For these reasons, the unlawfulness of the processing of personal data carried out by the Company is noted, in violation of the

principles of integrity and confidentiality and of the obligations of the data controller in terms of data security and impact assessment on data protection (5, par. 1, letter f), 32 and 35 of the Regulation) as well as art. 75 of the Code, which is without prejudice to the specific sector provisions contained in the d.P.C.M. 8 August 2013 and in the emergency regulations referred to above, in the terms set out in the motivation.

In this context, considering, in any case, that the conduct has exhausted its effects and that measures have been adopted to remedy the violation of personal data notified to the Authority and to prevent similar violations in the future, the conditions are not met. 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, par. 1, lett. f), 32 and 35 of the Regulations, as well as art. 75 of the Code, caused by the conduct put in place by the Company is subject to the application of a pecuniary administrative sanction pursuant to art. 83, par. 4, lett. a) and par. 5, lett. a) of the Regulations (see Article 166, paragraph 2, of the Code).

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

The aforementioned administrative fine imposed, depending on the circumstances of each individual case, must be determined in the amount taking into account the principles of effectiveness, proportionality and dissuasiveness, indicated in art. 83, par. 1, of the Regulation, in light of the elements provided for in art. 83, par. 2, of the Regulation in relation to which it is noted that:

- the treatments carried out by the Company subject to this provision concern data on the health of numerous interested parties, although the violation concerned only two interested parties (Article 83, paragraph 2, letter a) and g) of the Regulation);
- the Company promptly took charge of the problem that emerged in the violation of personal data, which was followed by the identification of specific measures (Article 83, paragraph 2, letter c) and d) of the Regulation);
- the holder has demonstrated a high degree of cooperation (Article 83, paragraph 2, letter f) of the Regulation);

- no complaints or reports have been received to the Guarantor on the incident and there are no previous relevant violations committed by the data controller, nor have measures previously been ordered pursuant to art. 58 of the Regulations (Article 83, par. 2, letter i) of the Regulations);

- the facts of the violation occurred in the context of the public health activities carried out by the Company at a particularly critical moment in the current emergency context in which the need to urgently activate the screening activity was matured, guaranteeing at the same time, an orderly and safe management of the influx of people (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 pecuniary sanction provided for by art. 83, par. 5, lett. a) of the Regulations, to the extent of 14,000.00 (fourteen thousand) for the violation of Articles 5, par. 1, lett. f), 32 and 35 of the Regulations, as well as art. 75 of the Code, as a pecuniary administrative sanction, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary sanction of the publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Guarantor Regulation n. 1/2019, also in consideration of the type of personal data subject to unlawful processing.

Finally, it is noted that the conditions set out in art. 17 of Regulation no. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

WHEREAS, THE GUARANTOR

declares the unlawfulness of the processing of personal data carried out by the Marche Region Health Authority, for the violation of Articles 5, par. 1, lett. f), 32 and 35 of the Regulations, as well as art. 75 of the Code.

ORDER

pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, to the Marche Region Health Authority, with registered office in Ancona, via Oberdan 2 - 60122, VAT number: 02175860424, in the person of the pro-tempore legal representative, to pay the sum of € 14,000.00 (fourteen 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 Marche Regional 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 € 14,000.00 (fourteen 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, January 13, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Ghiglia

THE SECRETARY GENERAL

Mattei