[doc. web no. 9871846]

Injunction order against the Campania Region - 1 December 2022

Register of measures

no. 42/2023

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, prof.ssa Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, components, and the cons. Fabio Mattei, general secretary;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as well as on the free circulation of such data and repealing Directive 95/46 /CE-General Data Protection Regulation (hereinafter "Regulation");

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data (hereinafter the "Code");

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

HAVING REGARD to the documentation in the deeds;

GIVEN the observations made by the Secretary General pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web no. 1098801;

Speaker the lawyer Guido Scorza;

WHEREAS

1. The personal data breach notified, the complaint, the reports and the preliminary investigation carried out

The company SO.RE.SA. Spa (hereinafter also only Company or SO.RE.SA.), has notified this Authority, pursuant to art. 33 of the Regulation, a violation of personal data concerning unauthorized access to the contact details (telephone number and email) of "citizens of the Campania Region who have already joined the vaccination campaign" (deed of notification of the XX).

In the aforementioned notification, the Company qualified itself as data controller and indicated, among the subjects involved in the same, the company Enterprise Services Italia S.r.l., as data controller.

The Company has represented, also in the context of subsequent integrations pursuant to art. 33, par. 4 of the Regulation, in particular that "from the technical checks carried out by the Data Processor, the unauthorized accesses to information system data for the phase of joining the Covid19 vaccination campaign in the Campania Region took place through specific IT tools that require a specific competence and a specific intent to violate, directly accessing internal functions of the application (API). Normal access via browser to the prepared interface would not have allowed unauthorized access" and that "the possibility of unauthorized access to data was inhibited starting from 15 February" (note of the XX).

At the time of notification, the Company declared that the violation involved five "citizens of the Campania Region who have already joined the vaccination campaign" and subsequently specified that, from the technical checks carried out, "the unauthorized accesses occurred between XX and XX and concerned a total of 12 users with regard to the telephone number and e-mail address entered during registration. For a single user of the 12, possible access to the medical history form was detected (again in relation to the data entered by the user during registration)". In particular, the medical history file contained the information required by the Ministry of Health (https://www.salute.gov.it/imgs/C_17_pagineAree_5452_3_file.pdf ) (note of the XX and note of the XX).

SO.RE.SA. he also specified that "there are no certain criteria that make it possible to identify the personal data for which there has been an incorrect access attempt which has led to illegitimate access to information relating to the state of adherence to the vaccination campaign by means of the message of error" and that "there are no elements suitable to believe that an overwriting and/or cancellation of the personal data subject to the violation has been carried out and that, therefore, the nature of the violation can only be limited to the loss of confidentiality" (note of the XX ).

With reference to the security measures adopted with respect to the processing of the data in question, the Company represented that "considering the absolute necessity and urgency to implement the Strategic Plan with the immediacy required by the current emergency context, it is deemed that the measures adopted, with a view to balancing the right to privacy and public health, and by virtue of the number of data subjects, the nature, number and degree of sensitivity of the personal data violated, have been suitable for guaranteeing the necessity and urgency to allow the over 80s category to register and subsequently adhere to the vaccination campaign as soon as possible, taking into account the operational difficulties

associated with the management of authentication via the health card of the aforementioned category. In confirmation of the temporary nature of the choice adopted, it is confirmed that the access mode with greater control was immediately restored precisely because the system implemented had already been implemented in this sense" (note of the XX).

Subsequently, the Company also represented "that the inconsistencies between the tax code and the valid health card in the regional registry of the patients and the data entered by the user during access are recorded - by design choice, as a precautionary control measure subsequently to the request for modification of the user authentication method - within the database, also in order to allow and/or facilitate subsequent security analyses. This made it possible to analyze and delimit the set of data potentially involved in the violation found. The health card numbers that were not formally correct were identified, present within the set of data identified and, therefore, attributable to unauthorized access. In this sense, it should be noted that the application is equipped with a control function, designed to prevent the inclusion of information that is not formally correct in the field dedicated to the health card" (note of the XX).

With reference to the measures adopted to remedy the personal data breach and to those adopted to mitigate the possible negative effects of the same against the interested parties, the Company represented that:

- "as part of the investigations conducted to ascertain the extent of the violation, it proceeded - in the first place - to delimit the set of data potentially involved in the violation, identifying the inconsistencies for the tax code between the valid health card in the regional level of the assisted and the one entered by the user during access. These inconsistencies are, in fact, recorded - by design choice - within the database, also for the purpose of allowing and/or facilitating subsequent security analyses";
- “has identified the health card numbers that are not formally correct, present within the set of data identified and, therefore, attributable to unauthorized access. In this sense, it should be noted that the application is equipped with a control function, designed to prevent the inclusion of information that is not formally correct within the field dedicated to the health card";
- “identified the 12 personal data involved in the violation. Once this set of data had been defined, the Company found that only 3 of the aforementioned 12 personal data contained information within the medical history form, the compilation of which, among other things, is optional. With reference to these 3 personal data, the Company noted, only in one case, the completion of the anamnestic form at a time prior to the date of the last unauthorized access. Consequently, it is reasonable to believe that the violation could have potentially involved only this anamnestic record" (note of the XX).

With regard to the measures adopted to prevent similar violations in the future, the Company in the aforementioned note to the

XX, declared that it had:

a) "restored the level of control originally implemented and modified at the time at the request [... of the Campania region] in the face of organizational problems;

b) modified the error message generated by the application making it suitable not to produce any information on the interested party;

c) modified the API in such a way that they do not return information directly or indirectly attributable to the interested party;

d) planned to launch a system security verification activity through penetration tests, which will be performed both on the web interface and on the application endpoints";

and, in the subsequent note of the XX, that:

e) "following what emerged from the checks [...], we confirm that we have taken steps to modify the error message generated by the application, making it suitable not to produce any information on the data subject. By invoking the endpoint API https://api-sanita.cdp-sanita.soresa.it/cv19ade/v1/associazione/create%E2%80%9D the returned JSON no longer provides useful information on the data subject";

f) "Enterprise Service Italia S.r.l. proceeded to carry out specific security tests (penetration tests and vulnerability assessments) on the platform affected by the data breach and, based on the results, a remediation plan was drawn up. It is also specified that the above tests were carried out in the pre-production area, mirroring the production area, and on all the endpoints related to the service, in addition to those subject to data breach".

With reference to the communication to the interested parties, the Company, at the time of the notification, then declared that the due assessments were "in progress" in this regard. Subsequently, with the XX note, the Company provided a copy of the communications sent to the data subjects involved on the XX date, in which it qualified itself as data controller.

In conjunction with the investigation of the aforementioned notification of violation, following the presentation of a complaint and certain reports, this Office has launched specific investigation activities relating to the processing of personal data, also relating to the state of health of the interested parties, carried out by of the Campania Region in the context of online services relating to the execution of Sars Cov 2 tests and the administration of anti Covid-19 vaccines.

In particular, in examining the models used to provide data subjects with the information pursuant to articles 13 and 14 of the Regulation and further documentation, conflicting indications were found regarding the owner of the treatments currently in

question (articles 4, 13, and 24 of the Regulation). More specifically, it was found that, although the aforementioned models concerned the same treatments, they indicated the ownership of the treatment in a different way, referring, in some cases, to the Region and in others to SO.RE.SA.

Given this, on the basis of what is indicated by the Regulation and by the sector legislation adopted with reference to the prevention and containment actions of the Sars Cov 2 infection, the Office, in detecting critical aspects relating to the correct identification of the holders of the aforementioned treatments and the necessary designations as data processors of the subjects used by the data controllers, promoted a meeting with the Campania Region and the company SO.RE.SA, which took place remotely on the XX (note of the XX, prot. n XX).

As part of the aforementioned meeting, what was already indicated in the documents was represented and in particular that the definition of roles in the field of personal data protection, established in Commissioner's Decree n. 26 of 22.9.2019, identified SO.RE.SA. as "Data Controller" or Owner of the processing of personal data in the health sector, pursuant to art. 4, par. 1, no. 7 of EU Regulation 679/2016 GDPR. On that occasion, the Campania Region expressed its intention to adopt a new resolution regarding the definition of the roles of the processing of personal data carried out by it.

With a note dated XX, the personal data protection officer of the Region stated that “the Campania Region will redefine the roles of Data Controller and Data Processor with So.Re.Sa. S.p.A., surpassing the decree of the Commissioner ad Acta n. 26 of 22.02.2019".

Subsequently, with a note dated XX, the Region sent resolution no. 480 of 4 November 2021 of the Regional Council with which the roles of owner and manager were redefined with reference to the processing of personal data covered by this provision.

2. The alleged violations

In relation to what emerged from the documentation in the records, the Office notified the Campania Region, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation, inviting the aforesaid owner to produce defense writings or documents to the Guarantor or to ask to be heard by the Authority (art. 166, paragraphs 6 and 7, of the Code; as well as art. 18, paragraph 1, of law no. 689 of 11/24/1981) (note of the XX, prot. n. XX).

In particular, the Office found that the personal data breach described above was brought to the attention of the Authority and

the interested parties by the company SO.RE.SA. as independent data controller despite the fact that the violation concerned treatments not falling within the scope of the Company's ownership, but rather treatments relating to public health initiatives connected to the implementation of the anti Covid-19 vaccination campaign which fall within the scope of the Campania Region .

It was also found that the web application for joining the anti Covid-19 vaccination campaign allowed, albeit for a limited period of time (one week), the consultation of certain personal information of regional health system patients simply entering the tax code and a 20-digit string, even if it does not correspond to the relevant health card number.

In particular, it was found that, up to the date of the twentieth, by entering the tax code of a client of the Region who had already joined the vaccination campaign and, as a health card number, a random string of 20 digits, the aforementioned web application showed a message ("Attention - You have already joined the vaccination plan") from which it was possible to infer information about the successful adherence to the anti-Covid 19 vaccination campaign of the person in charge of the tax code.

Furthermore, even the API with the endpoint "https://api-sanita.cdp-sanita.soresa.it/associazioneben/v1/associazione/create", invoked by the user's browser, returned, in JSON format, some information concerning adherence to the vaccination campaign of the patient (see element called "message", containing the fields "CF", "idRichiestaVaccino" and "stato").

It was then noted that as of the twentieth date, by entering the tax code of a client of the Region who had already joined the vaccination campaign and a string of 20 digits which is formally correct but does not necessarily correspond to the client's health card number, despite the mentioned web application showed a message with generic content ("Warning - Information not currently available"), the API with endpoint "https://api-sanita.cdp-sanita.soresa.it/cv19ade/v1/associazione/create" , invoked by the user's browser, still returned the above information in JSON format.

In the light of these elements, the Office, with note dated XX, prot. no. XX, notified the Campania Region, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions referred to in article 58, par. 2, of the Regulation, inviting the aforesaid owner to produce defense writings or documents to the Guarantor or to ask to be heard by the Authority (art. 166, paragraphs 6 and 7, of the Code; as well as art. 18, paragraph 1, of law no. 689 of 11/24/1981). In particular, the Office highlighted that the methods of accessing the services then offered by the booking platform for the anti Covid-19 vaccines did not comply with art. 5, par. 1, lit. f), and in art. 32 of the Regulation as inadequate to guarantee the confidentiality of information on a permanent basis, also relating to the state of health of the interested parties.

The Office also noted the violation by the Campania Region of the obligations of "data protection from the design stage" and "data protection by default" referred to in the aforementioned art. 25 of the Regulation to the extent that it was ascertained that at the time of defining the characteristics of the web application for joining the anti Covid 19 vaccination campaign and subsequently during its use, it did not proceed with the implementation of technical measures aimed at effectively implementing the principles inherent in the processing of personal data, with particular reference to that of integrity and confidentiality (Article 5, paragraph 1, letter f) of the Regulation).

Finally, the incorrect attribution by the Campania Region of the ownership of the processing carried out through the aforementioned portal and the consequent erroneous attribution of the tasks and responsibilities of the various subjects involved in the processing also in relation to the obligations regarding data breach was found personal and security of the treatment in violation of the principle of "lawfulness, correctness and transparency" of the treatment pursuant to art. 5, par. 1, lit. a) of the Regulation also taking into account that information has been prepared containing conflicting information regarding these aspects of the processing.

Given this, the violation of the principles applicable to the processing of personal data pursuant to art. 5, par. 1, lit. a) and f), of the Regulation and of the following articles 25, 32, 33 and 34. The violation of the aforementioned provisions makes the administrative sanction provided for by art. 83, par. 4, lit. a) and par. 5, letter. a) of the Regulation

As part of the sanctioning procedure initiated with the aforementioned note of the XX, the Campania Region requested to be heard at a hearing (held on the XX date). On that occasion, the party - reserving the right to produce a specific report within 15 days - underlined that "all the actions connected with the integration of the regional register of patients shared the objective of guaranteeing that the regional health and hospital authorities could operate on a single registry that would give greater certainty on the services provided".

With a subsequent note of the XX (prot. n. XX), in addition to what has already emerged during the preliminary investigation, the Region highlighted in particular that:

- "in the emergency context in which the Campania Region found itself, the collection and use of data, and in particular those relating to health, have acquired a fundamental role in the action to combat the pandemic. The protection of personal data, in the time of the Covid-19 pandemic, contemplates limitations necessary to guarantee public health, through criteria of proportionality, precaution and temporariness. The decree-law of 9 March 2020, n. 14 containing Urgent provisions for the

strengthening of the National Health Service in relation to the COVID-19 emergency, published in the Official Gazette no. 62, on 9 March 2020, and in force since 10 March 2020, allows for a regulation for the protection of personal data based on art. 9, par. 2 lett. i) of the GDPR”

- "with reference to the implemented/planned remedial measures was:

- restored the level of control originally implemented and modified at the time at the request of the owner in the face of organizational problems;

- modified the error message generated by the application making it suitable not to produce any information on the interested party;

- modified the APIs so that they do not return information directly or indirectly attributable to the interested party;

- carried out system security verification activities through penetration tests".

- "the maximum collaboration with the Authority was ensured from the beginning of the proceeding and all the useful elements were provided to remedy the violation and mitigate its possible negative effects"

- "at 20 of the XX we became aware of the violation, at 21:30 of the same day a report was sent to the Postal Police, on the XX day a communication was made pursuant to art. 33 of the Regulation”;

- the Regional Council, as anticipated in the preliminary investigation phase to the Guarantor's Office, "with DGR 480 of 2021, notified to the Authority, proceeded to establish the Ownership of the Campania Region and to appoint So.Re.Sa. as responsible for the treatment”;

- "at the same time as the approval of the joint deed, the information has been adapted, the current legislation applies for the return";

- (...) "considering the absolute necessity and urgency to implement the Strategic Plan with the immediacy required by the current emergency context, it is believed that the measures adopted, with a view to balancing the right to privacy and public health, and by virtue of the number of data subjects, the nature and degree of sensitivity of the personal data violated, have been suitable for guaranteeing the need and urgency to allow the over 80 category to register and subsequently adhere to the vaccination campaign as soon as possible, taking into account the operational difficulties associated with the management of authentication via the health card of the category indicated above. In confirmation of the temporary nature of the choice adopted, it is confirmed that the access mode with greater control was immediately restored, precisely because the system

created had already been implemented in this sense". In any case, the implemented/planned initiatives were promptly activated:

- restored the level of control originally implemented and modified at the time (...) due to organizational problems;
- modified the error message generated by the application making it suitable not to produce any information to the interested party;
- modified the APIs so that they do not return information directly or indirectly attributable to the interested party;
- planned to start a security verification activity of the penetration test system, which will be carried out both on the web interface and on the application end points".

With reference to the principle of transparency, the Region highlighted that "this aspect should be mitigated by the fact that in 2019 the Campania Region was commissioned by the central government for the Plan for the return from health services. Precisely by virtue of the Resolution of the Council of Ministers of 10 July 2017, Acta vii [...] it was necessary to adopt the decree of the Commissioner ad Acta n. 26 of 22 February 2019 approved by the accompanying Ministries.

This provision arose from a specific request by Sogei as an administrative process that led to the establishment of regional registry offices with a clear indication of the ownership of the legal entity that carries out the processing. The only condition for being able to provide the Health Card System with the necessary information on Campania patients.

Consequently, the information produced could not be compliant with the dictates of the aforementioned decree of the Commissioner ad Acta. Then promptly adapted to the provisions of the new DGR 480/2021 (...) ".

3. Applicable legislation

The processing of personal data must take place in compliance with the applicable legislation on the protection of personal data and, in particular, with the provisions of the Regulation and of the Code.

In particular, it should be noted that, pursuant to the Regulation, "data relating to health" are considered: personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information relating to his or her state of health” (Article 4, paragraph 1, no. 15 of the Regulation). Recital no. 35 of the Regulation then specifies that 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 or her for health purposes”.

It should also be noted that pursuant to the Regulation, personal data must be "processed 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 (Article 5, paragraph 1, letter f), of the Regulation).

Based on this principle, the art. 32 of the Regulation provides that, "taking into account the state of the art and implementation costs, as well as the nature, object, context and purposes of the processing, as well as the risk of varying probability and severity for 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 appropriate level of security, particular account is taken of the risks presented by the processing which derive in particular from the accidental or illegal destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed" (par. 2).

Furthermore, it is noted that, based on the principle of "data protection from the design" (Article 25, paragraph 1, of the Regulation), the data controller must adopt adequate technical and organizational measures to implement the principles of data protection data (art. 5 of the Regulation) and must integrate the necessary guarantees in the processing to meet the requirements of the Regulation and protect the rights and freedoms of the interested parties. This obligation also extends to treatments carried out by means of a data controller. In fact, the processing operations carried out by a manager should be regularly examined and evaluated by the controller to ensure that they continue to comply with the principles and allow the controller to fulfill the obligations set out in the Regulation (see "Guidelines 4/2019 on Article 25 Data protection by design and by default", adopted on 20 October 2020 by the European Data Protection Board, spec. points 7 and 39).

The data controller must, also in compliance with the principle of "data protection by default" (Article 25, paragraph 2, of the Regulation), make choices such as to guarantee that only the treatment strictly necessary for achieve a specific and lawful purpose. This implies that, by default, the data controller must implement measures that guarantee that "personal data are not made accessible to an indefinite number of natural persons, without the intervention of the natural person" (see "Guidelines 4/ 2019 on article 25 Data protection from design and by default", cit., spec. points 55, 56 and 57).

The art. 33 of the Regulation establishes that "in the event of a personal data breach, the data controller shall notify the competent supervisory authority pursuant to article 55 of the breach without unjustified delay and, where possible, within 72

hours from the moment in which become aware, unless the personal data breach is unlikely to present a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it is accompanied by the reasons for the delay" (par. 1).

The art. 34 of the Regulation establishes that "when the violation of personal data is likely to present a high risk for the rights and freedoms of natural persons, the data controller communicates the violation to the interested party without unjustified delay" (par. 1) and that "the communication to the interested party referred to in paragraph 1 of this article describes in simple and clear language the nature of the personal data breach and contains at least the information and measures referred to in article 33, paragraph 3, letter b), c) and d)" (par. 2).

Furthermore, the Regulation provides that personal data are "processed in a [...] transparent manner in relation to the interested party ("lawfulness, correctness and transparency")" (Article 5, paragraph 1, letter a)) and that " the data controller adopts appropriate measures to provide the interested party [...] with the communications referred to [...] in Article 34 relating to the processing in a concise, transparent, intelligible and easily accessible form, with simple and clear language" (art. 12, paragraph 1).

4. Conclusions

The aforementioned personal data breach was brought to the attention of the Authority and the interested parties by the company SO.RE.SA. as independent data controller. In the light of what is documented in the deeds and what is indicated by the Region in the aforementioned resolution no. 480 of 4 November 2021, it is confirmed that the aforementioned violation is not attributable to the processing activities that fall within the scope of the aforementioned Company, as it concerned treatments relating to public health initiatives connected to the implementation of the anti-Covid vaccination campaign. 19 which fall under the ownership of the Campania Region. In the light of the foregoing, the details of a violation of the obligations pursuant to articles 33 and 34 of the Regulation by the Campania Region.

The incorrect attribution of the ownership of the treatments carried out through the aforementioned portal and the consequent erroneous assignment of the tasks and responsibilities of the various subjects involved in the treatment also in relation to the obligations regarding the violation of personal data has led, as noted by the Office in cited note of the XX, also the violation by the Campania Region of the principle of "lawfulness, correctness and transparency" of the treatment pursuant to art. 5, par. 1, lit. a) of the Regulation especially with reference to the information provided to the interested parties who have been

contradictory regarding these aspects of the treatment.

In the light of the documentation in place, it is also confirmed that the procedures for accessing the services offered by the Campania Region's booking platform for anti-Covid-19 vaccines (https://associazionevaccinazioni.soresa.it/associazione/cittadino) do not comply with the aforementioned provisions pursuant to art. 5, par. 1, lit. f), and in art. 32 of the Regulation, resulting inadequate to guarantee the confidentiality of information on a permanent basis, also relating to the state of health of the interested parties.

The aforementioned methods of access also resulted in the violation by the Campania Region of the obligations of "data protection from the design stage" and "data protection by default" referred to in the aforementioned art. 25 of the Regulation to the extent that it is demonstrated that at the time of defining the characteristics of the web application for joining the anti Covid 19 vaccination campaign and subsequently during its use, the Region has not implemented technical measures aimed at effectively implementing the principles inherent in the processing of personal data, with particular reference to that of integrity and confidentiality (Article 5, paragraph 1, letter f) of the Regulation).

On these bases, taking into account the statements collected during the investigation - and considering that, unless the fact constitutes a more serious crime, whoever, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces deeds or documents falsified responds pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the duties or the 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 the act of initiation of the procedure, since none of the cases provided for by art. 11 of the Regulation of the Guarantor n. 1/2019.

For these reasons, the preliminary assessments of the Office are confirmed and the illegality of the processing of personal data carried out by the Campania Region is noted in violation of the principles of lawfulness, correctness and transparency, integrity and confidentiality and related obligations of security, data protection from the design and by default and in violation of the obligations under Articles 33 and 34 of the Regulation (articles 5, paragraph 1, letters a) and f), 25, 32, 33 and 34 of the Regulation).

The violation of the aforementioned provisions also renders the administrative sanction envisaged by art. 83, par. 4 and 5 of the Regulation, pursuant to articles 58, par. 2, lit. i) and 83, par. 3 of the same Regulation.

5. Adoption of the injunction order for the application of the pecuniary administrative sanction and accessory sanctions (articles

58, paragraph 2, letter i and 83 of the Regulation; article 166, paragraph 7, of the Code)

The violation of the articles 5, par. 1, lit. a) and f), 25, 32, 33 and 34 of the Regulation, caused by the conduct of the Campania Region, is subject to the application of the administrative fine, pursuant to art. 83, par. 4, lit. a) and 5, lett. a) of the Regulation.

The Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, has the power to "impose a pecuniary administrative sanction pursuant to article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, according to the circumstances of each single case" and, in this context, "the College [of the Guarantor] adopts the injunction order, with which it also orders the application of the ancillary administrative sanction of its publication, in whole or in part, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code" (art. 16, paragraph 1, of the Guarantor's Regulation no. 1/2019).

The aforementioned pecuniary administrative sanction imposed, according to 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 the light of the elements provided for by art. 83, par. 2 of the Regulation. In relation to the violation of personal data notified by the data controller, pursuant to art. 33 of the Regulation, and based on the results of the investigation carried out, it is observed that:

- the violation involved a small number of interested parties and that with reference to a single interested party, it also involved access to the medical history file containing detailed health information;
- the Company has implemented technical measures suitable for preventing the recurrence of similar events, adapted to the state of the art and to the previous indications of the Authority (provision of May 13, 2021 web doc. 9674151);
- the circumstance that the definition of roles in matters of personal data protection had been established in Commissioner's Decree no. 26 of 22.9.2019 which had identified SO.RE.SA. as "Data Controller" does not constitute a condition exempting from the obligation for the data controller (in this case the Campania Region) to verify the treatments that pertain to its institutional duties and functions;
- the events subject to notification and reports took place in a moment of exceptional gravity, caused by the pandemic emergency from Covid-19 which also led to the declaration of a state of emergency with a resolution of the Council of Ministers of 31 January 2020;
- the Region promptly amended the regional legislation relating to the personal data protection roles of the Region itself and of

SO.RE.SA and the information on the processing of personal data;

- the Region proved to be cooperative throughout the preliminary and procedural phase;

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 4 letter. a) and 5, lett. a) of the Regulations, in the amount of € 10,000 (ten thousand) for the violation of articles 5, par. 1, lit. a) and f), 25, 32, 33 and 34 of the Regulation, as a pecuniary administrative sanction withheld, pursuant to art. 83, par. 1 and 3, of the Regulation, effective, proportionate and dissuasive.

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

Finally, it should be noted that the conditions pursuant to art. 17 of regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

ALL THIS CONSIDERING THE GUARANTEE

declares the illegality of the processing of personal data carried out by the Campania Region, for the violation of articles 5, par. 1, lit. a) and f), 25, 32, 33 and 34 of the Regulation in the terms indicated in the justification.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code by the Campania Region, with registered office in via S. Lucia, n. 81, chap. 80132, tax code 800.119.906.39, to pay the sum of €10,000 (ten thousand) as an administrative fine 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 fine imposed;

ENJOYS

to the aforementioned Region, 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 (ten thousand) according to the methods indicated in the annex, within 30 days of notification of this provision, under penalty of adopting 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 entire publication of this provision on the website of the Guarantor and

believes that the conditions set forth in art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

Pursuant to art. 78 of the Regulation, of the articles 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision it is possible to lodge an 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 appellant resides abroad.

Rome, 1st December 2022

PRESIDENT

station

THE SPEAKER

Zest

THE SECRETARY GENERAL

Matthew