[doc. web no. 9883749]

Provision of 23 March 2023

Register of measures

no. 87 of 23 March 2023

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stazione, 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, containing provisions for the adaptation of the national legal system to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons with regarding the processing of personal data, as well as the free movement of such data and repealing Directive 95/46/EC (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 of the Guarantor n. 98 of 4/4/2019, published in the Official Gazette no. 106 of 8/5/2019 and in www.gpdp.it, doc. web no. 9107633 (hereinafter "Regulation of the Guarantor n. 1/2019");

HAVING REGARD to the documentation in the deeds;

HAVING REGARD TO the observations made by the general secretary 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 preliminary investigation.

On 21 April 2021, the Healthcare Authority of the Autonomous Province of Bolzano (hereinafter the "Health Authority") sent

this Authority, pursuant to art. 33 of the Regulation, a personal data breach notification concerning unauthorized access to the health documents of some patients determined by the vulnerability of the service relating to the Electronic Health Record (EHR) reachable via the URL https://fsse.civis.bz .it/fse.

In the aforesaid notification, the Healthcare Company represented that it did not consider itself the data controller since the "episode of violation of personal data strictly pertains to the technical implementation of the ESF instrument of South Tyrol and not to the healthcare assets of Ownership of the Healthcare Company of Alto Adige" and that "given the dispute between the two organizations, it was decided in any case to notify the episode".

Among the subjects involved in the processing of the personal data in question, the Healthcare Authority has indicated the company Informatica Alto Adige Spa (hereinafter "SIAG") - designated as data processor in 2010 - and the company Dedalus Italia S.p.a. (hereinafter "Dedalus") - also designated as data controller in 2018 - the latter "under the contract stipulated [... with] Informatica Alto Adige S.p.A. (on behalf of the Healthcare Authority of the Autonomous Province of Bolzano) for the supply of Xvalue software components in technological updating, in evolutionary maintenance of the current X1.V1 platform, for the creation of the Electronic Health and Social Health File of the Autonomous Province of Bolzano)" (see notification of April 21, 2021 and note of May 14, 2021).

Following the request for information from the Office of 4 May 2021 (prot. n. 24801), the Healthcare Company represented that "it does not directly manage any aspect of the ESF platform, which is in charge of SIAG/Dedalus; does not manage the Identity Management module, which is integrated into the MyCivis civic network; does not have direct visibility on the status of the consents of the interested parties, as the registration and management form is in the hands of SIAG; all access authorization checks are delegated to the SIAG platform side, as well as the complete view of the accesses made (access log)" (see note of May 14, 2021).

In response to the aforementioned request for information, the Autonomous Province of Bolzano (hereinafter the "Province") declared that "the violation occurred within a function of the application on which the FSE is active, due to application vulnerabilities of the software provided by Dedalus Italia Spa" noting that "MyCivis acts as the official portal of the Public Administration of South Tyrol to facilitate access by citizens and businesses to the information and services of the various public institutions present in the area. As such, the Data Controller is the Provincial Administration. MyCivis, with reference to the Electronic Health Record, acts as an "identity and access management" to authenticate the citizen to the service.

Informatica Alto Adige Spa is responsible for the development and updating of this portal as Data Processor on behalf of the Provincial Administration. As per the note dated 04.08.2021, the exploited vulnerability appeared to be at the application level, i.e., after the authentication service provided by MyCivis" and that "Informatica Alto Adige Spa operates on behalf of the Provincial Administration as data processor in accordance with established and regulated in the Framework Agreement dated 07.10.2018, approved with Provincial Government Resolution no. 675, for the activities envisaged in article 4, paragraph 1 of the provincial law n. 33/1982. With regard to the ESF, Informatica Alto Adige Spa carries out processing on behalf of the provincial administration" (see note of 14 May 2021).

Based on what was represented by the aforementioned Province and the aforementioned Health Authority, the Office requested information from SIAG (note of 4 June 2021), which, with regard to the violation of personal data, declared that:

"MyCivis acts as the official portal of the Public Administration of South Tyrol to facilitate the access of citizens and businesses to the information and services of the various public institutions present in the area. As such, the Data Controller is the Provincial Administration";

"MyCivis, with reference to the Electronic Health Record, acts as an "identity and access management" to authenticate the citizen to the service";

"for the Electronic Health Record MyCivis allows access only after authentication with TS/CNS and second level SPID as required by law;

"Informatica Alto Adige Spa is responsible for the development and updating of this portal as Data Processor on behalf of the Provincial Administration";

"as per the note of 04.08.2021, the exploited vulnerability appeared to be at the service provider level or, after the authentication service provided by MyCivis";

"the process of accessing the assisted persons within the Electronic Health Record has been structured in accordance with the provisions of the relevant Regulation (Prime Minister's Decree No. 178 of 29 September 2015 "Regulation on electronic health records");

"Following a valid and certified SPID authentication, it was possible to inject tax codes of other citizens into calls (API). Therefore, it was possible to recover a document belonging to another citizen, however this activity was regularly recorded within the monitoring systems (auditing) of the ESF. [...] From a technical point of view it was possible to invoke the

"getdocument" service by recalling a citizen's document using an authentication cookie that identifies a different person." (see note of 11 June 2021).

With regard to the violation of personal data, the SIAG company has specified that:

"Informatica Alto Adige Spa, having received notification of the violation, has proceeded to inform the Healthcare Company, in its capacity as Data Controller, of the violation. Once this violation was communicated, a comparison was made between the tax codes and the related accesses made ("log" analysis) within the FSE in the period from 01.01.2021 to 04.08.2021. The period of time within which the access control was carried out was thus defined taking into consideration the date on which the vulnerability was inserted within the application exploited for the violation, following an update from part of Dedalus Italia Spa agreed with the client, and the violation occurred. As per the note of 04.08.2021, there are no violations on personal data as a result of the aforementioned vulnerability, except for the events relating to the communication of the violation which took place on 04.06.2021. With regard to the tax codes referred to in point 1 of the note dated 04.08.2021, following further investigations to verify whether they have been subject to violations, we are communicating the confirmation of the violation. The total number of tax codes subject to violation is therefore equal to five";

"as per the note dated 04.08.2021, the vulnerability was resolved on the same evening of the communication by the reporting party. It is also represented that on 08.04.2021 the General Manager of Informatica Alto Adige Spa filed a complaint with the Postal Police of Bolzano for the facts covered by this communication. Informatica Alto Adige Spa, in its capacity as Data Processor, has also taken steps to inform the interested parties of the occurred violation of personal data, including the interested parties to whom the two tax codes still subject to assessment referred";

"The MyCivis portal offers, among the various functions, also that of "proxies". This function allows, through the appropriate procedures, to be able to operate on behalf of another legal or natural person different from the one who logged in. In the specific case of the violation, this procedure has not been violated. The breach, as described above, was caused at the service provider level (FSE application)";

"Informatica Alto Adige Spa has been appointed Data Processor by the Healthcare Company, as Data Controller. Informatica Alto Adige Spa as Data Processor has appointed Dedalus Italia Spa as further Data Processor as per the attachment for the processing of the Electronic Health Record" (see note of 11 June 2021).

At the time of notification, the Healthcare Authority declared that the violation involved 3 interested parties and, subsequently,

clarified that there were 5 interested parties involved, also on the basis of SIAG's declarations (see notification of 21 April 2021, integration of October 19, 2021 and SIAG note of June 11, 2021).

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 on the interested parties, the Healthcare Authority represented that:

a) "SIAG has launched an investigation with the provider of the Health Record infrastructure in order to remove the IT vulnerability";

b) "in the light of the SIAG communication [...] the reported vulnerability was already resolved around 7.15 pm on 6 April last." (see notification of April 21, 2021 and note of May 14, 2021).

As regards the measures taken to prevent similar violations in the future, the Healthcare Company stated that "the supplier reported that the vulnerability was resolved within 24 hours of the first report (April 06, 2021 around 19.15)" and, subsequently , that "SIAG has declared that it has taken the necessary measures to avoid the recurrence of similar episodes" (see notification of April 21, 2021 and integration of October 19, 2021).

On the basis of the above, with a note dated 1 March 2022 (prot. 13133), this Office made a notification of violation pursuant to art. 166, paragraph 5, of the Code to the Autonomous Province of Bolzano as it was found that the processing of personal data in question was carried out in a manner that does not comply with the principle of "integrity and confidentiality" (Article 5, paragraph 1, letter f), of the Regulation), by failing to adopt technical and organizational measures suitable for guaranteeing a level of security appropriate to the risk (Article 32 of the Regulation) and adequate, right from the design of the treatments carried out within the ESF, to implement the principles of data protection are effective and to integrate the necessary guarantees into the processing in order to meet the requirements of the Regulation and protect the rights of the interested parties, in violation of art. 25 of the Regulation, and also failing to notify the Guarantor of the violation of personal data that occurred, in violation of art. 33, par. 1, of the Regulation.

With a note dated 29 March 2022 (prot. n. 279657), the Province sent its defense briefs in which it represented, in particular, that:

"the unauthorized access to the health documents of some patients, subject of the personal data breach notified on 21.04.2021 by the South Tyrolean Health Authority (hereinafter "ASDAA"), was determined by a vulnerability of the related service to the Electronic Health Record (hereinafter "FSE"), the development of which is managed by Dedalus Italia Spa";

"this episode therefore peacefully pertains to the technical implementation of the FSE instrument which - as stated by the ASDAA itself during the notification - was entrusted by the latter to Informatica Alto Adige Spa (hereinafter "SIAG") and to Dedalus Italia Spa, identified pursuant to art. 28 of the Regulations, responsible and sub-manager respectively of the treatment relating to the supply of the Xvalue software components in technological updating, as well as evolutionary maintenance of the X1.V1 platform for the implementation of the FSE";

"in order to further clarify the role of the provincial administration, it seems useful to dwell on the role played by the ASDAA, as an instrumental body of the Autonomous Province of Bolzano (hereinafter "PAB"), also in the light of the provisions of art. 12 of the decree-law of 18 October 2012, n. 179, for which "The ESF is established by the autonomous regions and provinces", and of the decision-making polycentrism typical of PAB. The reference to the "autonomous province" corresponds in fact to a competence of a political nature, generically attributable to the PAB. Therefore, when the legislator indicates that the ESF is established by the autonomous provinces, the notion of autonomous province includes not only the provincial administration but also the instrumental bodies, especially those in charge of healthcare (ref: resolution no. 4830 of 12/18/2006, Provincial Law No. 7 of 5 March 2001 and Provincial Law No. 3 of 21 April 2017 which states that "The South Tyrolean Health Authority, hereinafter referred to as the Health Authority, is an instrumental body of the Province endowed with public juridical personality and management autonomy"). The normative reference to the "establishment" of the ESF expressly refers to the purposes connected with this institution ("The ESF is established ... for the purposes of: ..."), where a plurality of different decision-makers corresponds to each purpose and therefore a plurality of owners. In other words, the treatment referring to the institution of the ESF must be valued in the light of the logical-functional connection with the purposes listed in the art. 12, paragraph 2. The institutional competence in question does not therefore translate into ownership of all the treatments carried out by means of the ESF in the hands of the provincial administration. In this sense, the choice made by the legislator in paragraph 4 and following of the aforementioned article also bears witness, in which the purposes of processing as regards the content of the ESF and therefore the use of this instrument are attributed ex lege to specific owners. On the other hand, the ownership of the treatments pertaining to the ESF "container", both in its establishment and operational phases, should instead be determined, as far as the PAB is concerned, having regard to the deeds that concretely regulate the relations between the entities in various capacities involved, since there is no legal provision that regulates and clarifies, even indirectly, this aspect";

"ASDAA, SIAG and PAB have stipulated the agreement "for the assignment of tasks for the implementation of South Tyrolean

healthcare projects and for the activation of the services inherent to them within the CRO/FESR project 3- 1d-142” (attachment 1). This agreement, on page 1, identifies ASDAA as "owner of the South Tyrolean healthcare ICT system and responsible in its area for the design, acquisition and subsequent management and maintenance of the ICT system, the IT applications implemented and the related services". The agreement also specifies - page 2 point iii) - that "ASDAA as an instrumental body of the Province of South Tyrol intends to implement the Software called Platform X1V1 in its ICT system for South Tyrolean Healthcare in implementation of the aforementioned reuse";

"precisely in the appointment as data controller conferred by ASDAA on Dedalus we find the confirmation that SIAG acted "on behalf of" ASDAA, when it had concluded a contract with Dedalus precisely for the evolutionary maintenance of the X1.V1 platform";

"the Provincial Administration, despite having entrusted in a subsequent period (in particular during 2020) the task for further developments to SIAG (through its IT Department), which then re-entrusted the additional manager Dedalus Italia SpA (precisely because of the relationships already existing in 2017 and governed by the ASDAA), has not concluded a contract as data controller, but as a subject who, by virtue of the collaboration envisaged in the agreements signed between the parties as well as in the resolution of the Provincial Government mentioned above (n. 949 of 18.9.2018), performs tasks of an organizational and support nature, including economic, with respect to the project. It is understood that ASDAA is the body that pursues the purposes whose processing also finds expression in the FSE and which exercises the prerogatives of the data controller";

“Dedalus Spa immediately took care of the removal of the IT vulnerability on the recommendation of SIAG. The intervention of Dedalus Spa is therefore due to activities carried out on behalf of the owner, ASDAA";

"that it is a vulnerability relating to the FSE (service provider) application, also clearly emerges from the report sent by the citizen (Mr. XY) who exploited the security flaw. He promptly lists the steps performed to access the health data of other patients, which presuppose correct authentication to the MyCivis service. The vulnerability can therefore be exploited only after authentication (Annex 8). It is also specified that, as per the analyzes performed by SIAG, the vulnerability exploited by (Mr.XY) (as a real attacker), requires in-depth technical knowledge and is not an action that falls within the possibilities of users with basic and unevolved IT knowledge. It should be emphasized that this is therefore a targeted hacking of an IT system which required the possession of very specific technical knowledge and for which (Mr. XY) was reported to the competent

authorities on 04.09.2021 by SIAG, as from documentary evidence from this attachment";

"in the opinion of the writer, it is therefore undisputed that the perimeter of ownership of the ASDAA also extends to the application profiles of the FSE (for which it has in fact commissioned Dedalus Spa) and therefore to the patient id, not being in fact limited to the identification of the 'assisted in the provision of health services or in the association of metadata to health documents present in the EHR";

Furthermore, in the document "Project plan for the creation of the Electronic Health Record - Autonomous Province of Bolzano", Annex 3 to the aforementioned defense briefs, it is indicated that:

"the FSSE-AA project pursues the evolution and extension of the ESF in the Province, through a Program that defines and plans the activities that will be carried out by the Province, by the South Tyrolean Health Authority (hereinafter also ASDAA, or SABES , or Company) and by the public and private health and social care structures of the area, in accordance with the national "Regulations on ESF" (Annex 3 - Project plan for the creation of the Electronic Health Record of the Autonomous Province of Bolzano)";

"the FSSE-AA project is implemented by extending the SIS-FSE-ePRE system (Health Information System - FSE - Electronic Prescription) developed by the task entrusted by the IT Division 9 of the Province to Informatica Alto Adige S.p.A.";

"from an organizational and operational point of view, the project activities are centered on the two main actors, first of all the Province and then the ASDAA, which will jointly pursue the completion and evolution of the Provincial Health Information System, also on the basis of new needs and functions determined by the establishment of the provincial ESF as required by Law No. 221/2012 and its subsequent amendments (Law No. 98/2013)";

"the ownership and planning of the FSSE-AA project activities are held by the Health Division of the Province. The technical operational structure of the project made up of SIAG reports to this organization, which has the task of implementing and implementing the project on the territory. (...) On the ASDAA side, the IT interventions, for the creation of the Electronic Health Dossier (DSE) and for feeding the ESF, are set out in the "Plan for the strategic development of information technologies of the ASDAA"";

"as regards the control and monitoring of the project, as well as for other IT initiatives, the competence lies with the IT governance board of the Province";

"authentication to the system of health and social care workers of the provincial health system, as well as the patients, takes

place in the manner provided for by art. 64 of the "Digital Administration Code". Access is conveyed by the Civic Network of South Tyrol (the portal of the Public Administration) in the area of eGovernment services";

"On the provincial portal of the South Tyrolean Civic Network, in the area of eGovernment services, the following services will be integrated by July 2017: - Consent management; - ESF consultation; - Management of document blackouts; - Access consultation. (…) access to the ESF system will take place via the web portal of the Civic Network of South Tyrol in the eGovernment services area. The citizen (...) will be able to: - obtain a list of documents and information associated with it, which satisfy specific search criteria (the searches will be filtered according to the role of the requesting user); - select a document and display the content according to specific display profiles";

"the functions of feeding, searching, retrieving and updating documents will be guaranteed by the FSSE-AA infrastructure. The interfaces will expose all the necessary search, fetch, create and update operations. Similar capabilities will also be displayed via web front-end. Access to individual capabilities will be allowed on the basis of the type and role of the system user";

"furthermore, for the FSSE-AA system, periodic checks will be carried out on the authorization credentials and on the authorization profiles and, in general, on the security process adopted. In order to avoid the risk of unauthorized access to the ESF and ensure accuracy and continuity in the usability of the data, the Province will promptly notify the Guarantor of any violations in accordance with the requirements of the DPCM scheme attached to the March 2014 guidelines".

Finally, with reference to the roles assumed by the various subjects involved in the processing, the company SIAG, with a note dated 30 March 2022 (prot. n. 408), sent its defense briefs in reply to the notification of violation pursuant to art. 166, paragraph 5, of the Code, carried out by the Office in the context of the same investigation, representing that:

"To be precise, the supply chain is as follows: ASDAA (i.e. the South Tyrolean Health Authority) – SIAG – DEDALUS. SIAG is responsible for processing with respect to ASDAA, DEDALUS is with respect to SIAG";

"in turn, DEDALUS takes the role of data processor with respect to SIAG, i.e. is responsible for the data processor, as per the contract pursuant to art. 28 GDPR";

"SIAG is responsible for the treatment for ASDAA (in fact it acts "on behalf of the Healthcare Company…"); in this role, SIAG concluded a contract with DEDALUS; this contract determines the processing of personal data; therefore ASDAA designates DEDALUS as data controller".

2. Outcome of the preliminary investigation.

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

pursuant to the Regulation, "data relating to health" are considered personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information relating to his or her state of health (art. 4, par. 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 number, symbol or specific element attributed to a natural person to uniquely identify him or her for health purposes”;

the Regulation provides that personal data must be "processed in such a way as to guarantee adequate security (...) including protection, through appropriate technical and organizational measures, against unauthorized or unlawful processing and against accidental loss, destruction or damage («integrity and confidentiality»)” (Article 5, paragraph 1, letter f) of the Regulation). The Regulation also provides that the data controller, 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 freedoms of natural persons, must implement adequate technical and organizational measures to guarantee a level of security appropriate to the risk (Article 32 of the Regulation);

while considering that the multiple treatments carried out within the framework of the ESF fall under the ownership of several subjects pursuing different purposes, it should be noted that the processing activities with reference to which the violation occurred fall within the sphere of ownership of the Autonomous Province of Bolzano and not even from the Health Authority. Specifically, in fact, the violation does not appear to have been determined by an incorrect identification of the patient at the time of the provision of health services or by an incorrect association of the metadata to the health documents present in the EHR (processing activity of which the company is the owner), but from an incorrect functioning of the system that allows access to the documents contained in the ESF of the Autonomous Province of Bolzano, which falls precisely under the ownership of the latter. This is also evident from what is indicated in the documentation and in particular in the "Project plan for the creation of the Electronic Health Record - Autonomous Province of Bolzano". In fact, this document highlights that "the ownership and planning of the FSSE-AA project activities are held by the Provincial Health Department", which "as regards the control and monitoring of the project, as well as for other IT initiatives , the competence lies with the IT governance board of the Province” and that “the functions of feeding, searching, retrieving and updating documents will be guaranteed by the FSSE-AA infrastructure. The interfaces will display all the necessary search, retrieval, create and update operations”; the

violation appears, in fact, to have been determined by a vulnerability of the FSE application which allowed a subject authenticated to the MyCivis portal - of which the aforementioned Province is the owner - to view, select and open one or more documents of another client, even in the absence of a proxy, simply by modifying the patient_id parameter - containing the tax code - present in the URL used to display the list of documents available within the ESF and, therefore, within the perimeter of ownership of the aforementioned Province. This circumstance integrates a violation of personal data (art. 4, point 12, of the Regulation) that the Autonomous Province of Bolzano should have notified the Guarantor because, by allowing unauthorized access to the personal data of the clients stored within the ESF, it presented a risk to the rights and freedoms of the data subjects; this failure to notify integrates the details of a violation of the obligations pursuant to art. 33, par. 1, of the Regulation; in this regard, it should be noted that the aforementioned "Project plan for the creation of the Electronic Health Record - Autonomous Province of Bolzano" also provides that "in order to avoid the risk of unauthorized access to the EHR and guarantee accuracy and continuity in the usability of the data, the Province will promptly notify the Guarantor of any violations in accordance with the requirements of the DPCM scheme attached to the March 2014 guidelines".

the treatments carried out in the context in question require the adoption of the highest security standards in order not to compromise the confidentiality, integrity and availability of the personal data of hundreds of thousands of interested parties. This, also taking into account the purposes of the processing and the nature of the personal data processed, belonging to particular categories. On this basis, the security obligations imposed by the Regulation require the adoption of rigorous technical and organizational measures, including, in addition to those expressly identified by art. 32, par. 1, lit. from a) to d), all those necessary to mitigate the risks that the treatments present;

it is up to the data controller to "implement adequate and effective measures [and...] demonstrate the compliance of the processing activities with the [...] Regulation, including the effectiveness of the measures" adopted (cons. 74 of the Regulation), even if makes use of a manager for the performance of certain processing activities, to whom it must give specific instructions, also from a security point of view (cons. 81 and art. 32, par. 1, letter d), and 4, of the Regulation) . In fact, the controller remains responsible for implementing the appropriate technical and organizational measures to guarantee and be able to demonstrate that the processing is carried out in compliance with the Regulation (articles 5, paragraph 2, and 24 of the Regulation; see "Guidelines 7/2020 on the concepts of controller and processor in the GDPR", adopted by the European Data Protection Board on 7 July 2021, in particular, paragraph 2.1.4, point 41);

the modalities of access to the documents contained in the ESF of the assisted persons of the Autonomous Province of Bolzano were therefore not compliant with the provisions of the aforementioned articles 5, par. 1, lit. f), and 32 of the Regulation which establishes that the data controller and data processor must implement measures to "ensure on a permanent basis the confidentiality, integrity, availability and resilience of treatment systems and services" (par. 1, letter b)) and that in "evaluating the adequate level of security, particular account is taken of the risks presented by the processing which 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);

on the basis of 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 (article 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). For these reasons, the aforementioned access methods are also in contrast with the principles of "data protection from the design stage" pursuant to art. 25 of the Regulation. The Province has therefore failed to implement, right from the design of the treatments carried out in the context of the ESF, adequate technical and organizational measures, aimed at effectively implementing the principles of data protection and integrating the necessary guarantees in the treatment in order to meet the requirements of the Regulation and protect the rights of the interested parties, in violation of art. 25 of the Regulation.

3. Conclusions.

In the light of the assessments referred to above, taking into account the statements made by the owner during the preliminary investigation and considering that, unless the fact constitutes a more serious crime, anyone who, 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 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 deed of initiation of the proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

For these reasons, the unlawfulness of the processing of personal data carried out by the Autonomous Province of Bolzano in the terms set out in the justification, in violation of articles articles 5, par. 1, lit. f), 25, 32 and 33 of the Regulation of the Regulation.

In this context, considering that measures have been taken to overcome the vulnerabilities described above, the conditions for the adoption of the corrective measures pursuant to art. 58, par. 2, of the Regulation.

4. Adoption of the injunction order for the application of the pecuniary administrative sanction and accessory sanctions (articles 58, paragraph 2, letter i), and 83 of the Regulation; art. 166, paragraph 7, of the Code).

The violation of the articles 5, par. 1, lit. f), 25, 32 and 33 of the Regulation, caused by the conduct put in place by the Autonomous Province of Bolzano, is subject to the application of the administrative fine pursuant to art. 83, par. 4 and 5, of the Regulation.

Consider that 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, 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 the light of the elements provided for in art. 85, par. 2, of the Regulation in relation to which it is observed that:

the Authority became aware of the event following the notification of violation by the Healthcare Authority of the Autonomous Province of Bolzano (Article 83, paragraph 2, letter h), of the Regulation);

the treatment in question concerns data suitable for detecting information on the health of 5 subjects who were exposed to possible illegal access for about three months (from January to 6 April 2021) and, based on what was declared by the

Province, no further consequences for the interested parties and the data unlawfully viewed have not been used for other purposes or disseminated, nor is there any evidence of repercussions consisting of physical, material or immaterial damage to the interested parties (Article 83, paragraph 2, letter a) and g) , of the Regulation);

the Province has demonstrated a high degree of cooperation by striving to introduce, even in the concomitance of the emergency context, suitable measures to overcome the vulnerabilities highlighted above (art. 83, paragraph 2, letters c), d) and f), of the regulation);

the interested parties involved were informed of the violation by SIAG (by e-mail dated 14.05.2021) (art. 83, paragraph 2, letter c), of the Regulation).

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. 5, letter. a), of the Regulation, to the extent of 30,000 (thirty thousand) euros for the violation of articles 5, par. 1, lit. f), 25, 32 and 33 of the Regulation, as a pecuniary administrative sanction withheld, pursuant to art. 83, par. 1, 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 by 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 GUARANTOR

declares the illegality of the processing of personal data carried out by the Autonomous Province of Bolzano for the violation of the articles 5, par. 1, lit. f), 25, 32 and 33 of the Regulation in the terms referred to 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, to the Autonomous Province of Bolzano, tax code 00390090215, in the person of its pro-tempore legal representative, to pay the sum of 30,000 (thirty thousand) euros 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 Autonomous Province of Bolzano, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of 30,000 (thirty thousand) euros according to the methods indicated in the attachment, 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 publication of this provision in full on the website of the Guarantor and the annotation of this provision in the internal register of the Authority, provided for by art. 57, par. 1, lit. u), of the Regulation, of the violations and of the measures adopted in accordance with art. 58, par. 2, of the Regulation.

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, 23 March 2023

PRESIDENT

Station

THE SPEAKER

Zest

THE SECRETARY GENERAL

Matthew