[doc. web no. 9883731]

Provision of 23 March 2023

Register of measures

no. 86 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 Dr. Agostino Ghiglia;

WHEREAS

1. The preliminary investigation.

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

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.

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 14 May 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:

"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 customer, 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 violation, 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 a further Data Processor as per the attachment for the

treatment 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, supplement of 19 October 2021 and SIAG note of 11 June 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 21 April 2021 and integration of 19 October 2021).

Based on the above, with a note dated February 28, 2022 (prot. 13077), this Office made a notification of violation pursuant to art. 166, paragraph 5, of the Code to SIAG, which subsequently sent its defense briefs, in which it was represented that:

“the exclusive allocation of responsibility for the bug that concerns us does not lie with SIAG, but with the company Dedalus Italia s.p.a. (hereinafter "DEDALUS"), that this responsibility has amply admitted and documented";

"it should be highlighted, and constitutes a decisive point, that the attribution of the bug to DEDALUS is undisputed, has never been the subject of a dispute and was immediately recognized by the company in question";

"in particular, on April 7, 2021 the supplier (....) confirmed that it had been immediately alerted by SIAG on "April 6 [2021] at 10:00 am", i.e. the day after the bug was reported (...), and claimed to have "identified the problem in two services exposed by the portal backend"";

"ultimately, everything took place within the perimeter entrusted to DEDALUS and contracted with this company, as per documentary evidence";

"what were the security tests incumbent on the supplier and for what reasons these tests, although regularly carried out, did

not allow DEDALUS to intercept the bug, this company clarifies once again". "DEDALUS, that is, gives an account of having carried out the vulnerability assessments, but that this was not enough to avoid the presence of a bug, with this further confirming that the entire matter brought to the attention of this Authority took place within the operational perimeter, of verification (vulnerability assessment) and ultimately responsibility ("it did not trigger the launch of a Penetration Test, which could have identified it") of that company, not in that of SIAG";

with reference to the roles of the treatment, "the supply chain to be precise is the following: 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 positions itself with respect to SIAG in the role of data processor, that is, it is responsible for the 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";

"it is proven and documented that the bug occurred not at SIAG, but at DEDALUS, i.e. at the last link in the supply chain, and that in particular it escaped the vulnerability tests that DEDALUS had a precise legal obligation to carry out and which it declares in fact to have regularly performed";

"objective data is that the bug is exclusively and entirely attributable to an error by DEDALUS, which operated in the aforementioned capacity of data controller with respect to the IT procedures in which the electronic processing carried out by the said supplier necessarily takes the form".

On the basis of the investigative elements in the documents, the Office notified the company Dedalus, 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 company to produce defense writings or documents to the Guarantor or to ask to be heard by the Authority (article 166, paragraphs 6 and 7, of the Code; as well as article 18, paragraph 1, of law no. 689 of 11/24/1981) (note of 20 September 2022, prot. no. 49824).

In this deed, the Office represented that it had ascertained that the ESF of the Autonomous Province of Bolzano allowed a subject authenticated on the MyCivis portal to consult certain personal information of any patient in the Province by modifying the patient_id parameter -containing the tax code- present in the URL used to show the list of documents available within the EHR (https://fsse.civis.bz.it/fse/webapi/xds/getuserdocuments?patient_id = XXXXXXXXXXXX & date_from = YYYYYYYYY

&date_to=YYYYYYY&language= it&_=1617638439347).

In particular, from January to 6 April 2021, anyone, after passing the computer authentication procedures present in the MyCivis portal, could view, select and open one or more documents present in the EHR of another specific client, even in the absence of proxy, simply by entering the tax code of that client in the aforementioned patient_id parameter.

In the aforesaid notice of dispute, the Office therefore noted that the procedures for accessing the documents contained in the ESF of the clients of the Province did not comply with the provisions of 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).

With a note dated 18 October 2022, the Dedalus company sent its defense briefs, in which it represented in particular that:

"the Processing was carried out by Dedalus in the execution of the Contract, whose technical specifications (...) provided for a distribution of tasks and responsibilities between SIAG and Dedalus, also as regards the security aspects" and in particular, according to the aforementioned Specifications , SIAG had "the burden of carrying out vulnerability assessments and/or penetration tests";

“Dedalus had at the time implemented technical and organizational security measures relating to the processing pursuant to art. 32 of the Regulation", such as "by way of example and not limited to - the design of a correct process for user authentication and the related segregation of roles, encryption of communication channels, measures for access control and management and the tracking of events, the latter measure which has, among other things, made it possible to conduct an ex post analysis of the dynamics and consequences of the Data Breach”;

"the alleged violation had a limited duration, having been resolved within a few hours of its discovery", adopting "all measures aimed at mitigating its effects for the interested parties";

the violation derives "from an external intentional and malevolent action which exploited an unintentionally generated technical vulnerability of the computer system" and involved health data of "a few units" and therefore with an "extremely limited (a) (or) compared to the number of ESFs managed on behalf of the Province”.

2. Outcome of the preliminary investigation.

Having taken note of what is represented by the company Dedalus 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);

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);

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;

as emerged during the investigation, the data processing in question is carried out by the company in its capacity as data controller. Pursuant to art. 28 of the Regulation, in fact, the owner can also entrust a treatment to third parties who present sufficient guarantees on the implementation of technical and organizational measures suitable to guarantee that the treatment complies with the regulations on the protection of personal data ("data processors"). treatment");

therefore, the Regulation imposes certain obligations directly on the manager himself who, also on the basis of specific technical skills, must collaborate, also demonstrating proactive autonomy, in the adoption of adequate measures to "ensure on a permanent basis the confidentiality, the integrity, availability and resilience of the processing systems and services" (Article 32, paragraph 1, letter b), of the Regulation) and that in "assessing the adequate level of security, special account is taken manner of the risks presented by the processing which derive in particular from the destruction, loss, modification, unauthorized disclosure or access, in an accidental or illegal manner, to personal data transmitted, stored or otherwise processed" (art. 32, par. 2 of the Regulation).

In the case in question, the Dedalus company, due to its experience in the sector, was required to guarantee access to the documents in the ESF only to authorized parties, through the adoption of rigorous access control measures.

3. Conclusions.

In the light of the assessments referred to above, taking into account the statements made by the company Dedalus during the preliminary investigation and considering that, unless the fact constitutes a more serious offence, whoever, in a proceeding before the Guarantor, falsely declares or attests information or circumstances or produces false deeds or documents, it 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 in the defense briefs do not allow to overcome the findings notified by the Office with the deed of initiation of the procedure , since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

For these reasons, the illegality of the processing of personal data carried out by the Dedalus company is noted, in the terms set out in the justification, in violation of articles 5, par.1, lett. f), and 32 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, lett. f), and 32 of the Regulation, caused by the conduct of the company Dedalus Italia S.p.a., 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 have been exposed to possible illicit access for about three months (from January to 6 April 2021) (Article 83, paragraph 2, letter a) and g) , of the Regulation);

the Dedalus Italia company has demonstrated a high degree of cooperation by striving to introduce, even in the context of the emergency context, suitable measures to overcome the vulnerabilities highlighted above (Article 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) (Article 83, paragraph 2, letter c), of the Regulation);

on the basis of what was declared by the Province, no further consequences have been recorded for the data subjects and the

data unlawfully viewed have not been used for other purposes or disclosed, nor is there any evidence of repercussions consisting of physical, material or immaterial damage to the data subjects (art. 83, paragraph 2, letter a), 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 15,000 (fifteen thousand) euros for the violation of articles 5, par.1, lett. f) and 32 of the Regulation, as a pecuniary administrative sanction, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary sanction of 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 unlawfulness of the processing of personal data carried out by the company Dedalus Italia S.p.a. for the violation of the articles 5, par.1, lett. f) and 32 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 Dedalus Italia S.p.a., tax code 05994810488, in the person of its pro-tempore legal representative, to pay the sum of 15,000 (fifteen 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 aforementioned company, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of 15,000 (fifteen thousand) euros 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 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

guille

THE SECRETARY GENERAL

Matthew