SEE ALSO NEWSLETTER OF 30 MAY 2022

[doc. web n. 9771184]

Ordinance of injunction against the National Insurance Institute for Accidents at Work - April 28, 2022 *

Record of measures

n. 147 of 28 April 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

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

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

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

Having seen the documentation in the deeds;

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

Rapporteur the lawyer. Guido Scorza;

WHEREAS

1. Introduction.

On the twentieth, twentieth and twentieth centuries, the National Institute for Accident Insurance at Work (hereinafter, "INAIL"

or "Institute") notified the Guarantor, pursuant to art. 33 of the Regulation, three different violations of personal data, which occurred between 2019 and 2020, which concerned the online service called "Sportello Virtuale Lavoratori" (hereinafter, "Sportello Virtuale" or "SVL") - which provides a series of services aimed at working users - and which involved third parties viewing, on different days, the accident and occupational disease practices of other users.

The Virtual Desk allows, in particular, citizens who are victims of work accidents or occupational diseases, to view the status of their cases opened at INAIL as well as the measures issued by the Institute. Although the structured data processed cannot be traced back to particular categories, the measures that can be downloaded by the user usually also contain information on the state of health. The users registered on the portal with the “Citizen with dispositive credentials” profile (SPID, INPS PIN in the federation and INAIL credentials issued at the counter) are approximately 400,000 (see note of the XX, p. 1). These credentials allow access to the portal of the Institute which displays a series of services, in addition to the one subject to violation. The user can only view the accident or occupational disease files associated with their tax code and no dispositive operations are envisaged.

2. Personal data breaches.

More specifically, on the basis of the statements made by the Institute, both in the notification of personal data violations and in response to subsequent requests for information made by the Office, it appears that, between May 2019 and April 2020, some users have had the opportunity to view personal data, also relating to health, of other interested parties (also users of the service).

In particular, on the 20th the Institute notified the Guarantor of a personal data breach relating to the display, by a subject, on two different days, through the Virtual Desk, of accident and / or occupational disease practices relating to two other interested. In this regard, the Institute stated that such events would probably be attributable to an unspecified "configuration of the software and middleware infrastructures", assuming that it was "a contingent or at least very rare situation" and that "despite all the consultations of practices in the service in question are traced, the anomaly is such as not to leave information in the logging system "(see note of XX; see also notification of XX).

In order to remedy the violation of personal data, the Institute proceeded to suspend the "SVL" service and to adopt, before restoring its operation, technical and organizational measures aimed at preventing similar future violations (see note of the XX). He also specified that he had informed the two people affected by the violation episode, providing the Guarantor with a copy

of the communication sent on the XXth (see note of XX).

Subsequently, on the 20th, the Institute notified the Guarantor of a second violation of personal data, which occurred on 22 October 2019, specifying that:

"On the twentieth day, a lady (mother of an assisted worker) reports via email that after accessing INAIL's online services using her son's credentials, she has viewed files belonging to other people (she thought the son's homonyms). The user does not provide evidence (eg screenshots) of the data displayed but informs us that he has had access to practices that are not the responsibility of the child without, however, identification data attributable to other interested parties "(see note of XX, p. 4);

"The Workers Virtual Desk has shown a screen containing summary data of services erroneously associated with the name of the worker without, however, identification data of the other persons interested in the services" (see note of XX, p. 7);

the appropriate checks have been initiated, in order to ascertain their existence and determine the actual risk;

the preliminary analyzes have shown that "the personal information shown by the application in reference to the same name does not actually pertain to the practices of a possible user of the same name but to the practices of other non-identifiable users";

the additional details obtained by the user, together with the evidence of the analyzes carried out, allowed INAIL to become aware of the violation of personal data on November 27, 2019; however, it was "excluded that the data shown referring to homonymous or identifiable users" (see note of XX, p. 7);

"From the details received and the absence of other reports, it is assumed that these are the effects of a contingent or at least very rare situation. The display of personal and sensitive data by other people, even if they also belong to the category of injured or technopathic, undoubtedly constitutes a violation of the right to privacy. The damage that the individual could have had from this exposure, given the episodicity and randomness of the event, as well as the small population that could have viewed the data, seems modest, although it is undoubtedly an infringement of the sphere of rights "(see note of XX, p. 1);

“The violation of personal data involved a total of six“ non-identifiable ”data subjects and concerned, in particular, the“ type of practice (occupational disease or accident); iban and sums of benefits paid; state of processing of the file "(see note of the XX, p. 7).

Finally, on 24 April 2020, the Institute notified the Guarantor of a third violation of personal data - which always involved the Virtual Desk - following a report by a user who "on the evening of Wednesday 22 April 2020, between 21:00 and 21:50,

opening his INAIL position, he viewed the various measures with the related personal data of users of the La Spezia and Palermo offices, for which he provides two PDF files and associated screenshots "(v. note of the XX, p. 7). In particular, the Institute represented that:

- the violation concerned “data relating to accidents and / or occupational diseases: name, surname, type of practice (occupational disease or accident); information on the status and progress of the practice "referring to two interested parties and that the same was determined by a" process error that led to the presence in operation of the wrong version of the application "(see note of XX, pp. 5 and 7) ;

- "the seriousness of the violation is high as it is possible to download the documentation in PDF format containing information and particular personal data of other users" (see note of XX, p. 9);

- has communicated the violation of personal data to the interested parties involved, providing a copy of the communication sent (see note of XX, pp. 4 and 5).

3. The technical and organizational measures adopted.

With regard to the technical and organizational measures adopted to remedy the violation of personal data, the Institute stated that, following the violation notified on November 29, 2019 and to mitigate the possible negative effects on the data subjects, - also following the violation of personal data notified on May 16, 2019 - the following initiatives:

- “repeat the safety tests using up-to-date verification criteria and tools […]”;

- "Introduce additional logging mechanisms since it was found that, despite all the file consultations in the service in question are traced, the anomaly was such as not to leave information in the logging system [...];

- "activate a particularly analytical monitoring for the SVL service in order to understand the causes of the problem, should it recur, it being understood that the anomaly would be neutralized by the further control indicated below [...]";

- "in addition to the controls on the manipulation of user sessions already implemented on the services of the Institute, introduce a centralized module that performs consistency checks between session information, session cookies and the IP of origin of the requests, also allowing a raising of the tracking level "(see note of the XX, p. 2);

- downstream of these interventions, "however, a process error led to the presence in operation of the wrong version of the application, resulting in the subsequent violation referred to in the communication notified on 24 April 2020" and "from the moment of loading the corrected version of the 'application, the aforementioned logs have not detected further instances of the

problem and therefore, from the data available to date, the extent of the violation and the involvement of the interested parties is considered limited to what was communicated to the Authority "(see note of XX, p . 3).

With regard to the technical and organizational measures adopted to prevent similar personal data breaches in the future, the Institute stated that, in addition to the measures described above, it would also carry out "checks and audits in order to optimize the deployment process. In detail, a specific audit initiative has already been announced by the head of the competent Office in order to provide the necessary information to the Guarantor Authority for the protection of personal data in relation to a data breach report that occurred for the "Sportello Virtual Workers ", which will have the purpose of identifying the possible causes that generated the aforementioned violation and identify possible improvement actions in order to avoid the repetition of the event" (see note of XX, p. 3).

4. The preliminary investigation

In response to a request made by the Guarantor's Office (see note of the XX, in deeds), the Institute has:

provided the report containing the results that emerged from the execution of the internal audit activities regarding the event that took place on 22 April 2020 on the Virtual Desk;

specified that he had contacted the users who had access to third party data in order to request "more specifications about the occurrence of the anomaly and verbally provide the indications to prevent unauthorized data processing (eg illicit use, communication to third parties or dissemination) ", Also asking" to delete as soon as possible the data received erroneously without making further and improper use ";

prepared for this purpose a communication model, to be provided to any third parties to whom personal data may be transmitted in the future in an improper way, including indications to prevent unauthorized processing of data (see note XX, p. 2);

provided statistical data relating to the use of the "SVL" service starting from March 2020 (usually about 10,000 accesses / month), highlighting how "in the previous months, due to the aforementioned data breach events and subsequent deactivations of the functions involved in the problem in order to eliminate the risk exposure of the interested parties, the data do not provide significant indications of the trend and volume of use of the service "(see note XX p. 3).

With a note dated XX (prot. No. XX), the Office, on the basis of the elements acquired from the verifications carried out and the facts that emerged as a result of the investigation, notified the Institute, pursuant to art. 166, paragraph 5, of the Code, the

initiation of the procedure for the adoption of the measures referred to in art. 58, par. 2, of the Regulation, concerning the alleged violations of articles 5, par. 1, lett. a) and f), 6, par. 1, lett. e), 9, par. 2, lett. g), and 32 of the Regulations, as well as 2-ter and 2-sexies of the Code in the text prior to the changes made by the Legislative Decree. 8 October 2021, n. 139, applicable to the present case.

With the same note, the Institute was invited to produce defensive writings or documents to the Guarantor or to ask to be heard by the Authority (Article 166, paragraphs 6 and 7, of the Code, as well as Article 18, paragraph 1, of the l. November 24, 1981, n. 689).

With a note of the twentieth, the Institute presented its defense brief, declaring, in particular, that:

- “Overall, the […] violations resulted in: the display of personal data of 8 people (first and second violation event); viewing and downloading in PDF format of personal data of n. 2 people (third violation event) ";
- "INAIL immediately recognized a high level of severity for these events, implementing a series of additional security countermeasures aimed at reducing the impact and the future probability of occurrence. INAIL promptly notified the aforementioned personal data violations to the Authority and promptly informed the interested parties involved in the violations ";
- “[…] the incidental visualizations of personal practices by third parties have occurred following an accident. Therefore, in the case of an event by definition out of control and beyond the will of the Owner, there can be no regulatory support in this regard ";
- "[...] the application of state-of-the-art security countermeasures does not guarantee that problems or accidents will never occur; security is in fact a complex matter, not completely controllable and in continuous evolution. It follows that the occurrence of an accident is not sufficient to demonstrate that the planning and design of the countermeasures was not adequate with respect to the state of the art. In this regard, it is stated that there are no security countermeasures deriving from the risk analysis that have been identified but not implemented, nor security domains not considered ";
- "in particular, [...] the Institute: operates according to processes, using the ITIL V3 framework as a reference framework; has its own Information Security Management System (ISMS), ISO27001 certified since 2017; it has put in place technical and organizational security measures to protect the personal data that it processes on the basis of its institutional mission ";
- "the Institute operates in accordance with the provisions of the ISO27001 certified Information Security Management System

(ISMS), resulting to date among the few public administrations to have achieved this goal";

- "the SVL service in question has made use of and makes use of the same preventive and corrective countermeasures of systems such as that for ISI loans to companies or that for the management of accident reports, which have been certified for more than three years pursuant to the ISO-27001 standard and falls within the more general certification perimeter linked to the Institute's "Data Center";

- "at the process level INAIL uses, in its process model definition, the ITIL V3 framework as a reference framework, aimed at offering indications for the provision of quality IT services";

- "therefore," the SVL system was, like the other INAIL applications, subjected to functional tests, stress tests, accessibility tests and safety checks before each release into production, [and] managed in operation in compliance with the same operating procedures applied for services certified according to the ISO-27001 standard, in an environment protected from intrusions and constantly monitored, from a security point of view, by the Security Operations Center ";

- “the technical cause of the episodes is, to date, unknown, it has never been possible to replicate the malfunctions in a controlled environment, not even simulating high operating loads. It is believed that the cause may lie in undocumented behavior of the software platforms purchased by INAIL (operating systems, application servers, etc.), among other things included in a complex supply chain with high probability that the cause is in one of the supply chain systems , for which the Institute can only limit itself to regularly applying the corrective patches distributed by the relative suppliers ";

- "the sequence of the three incidents involving the SVL service does not therefore demonstrate the absence of adequate countermeasures, but the occurrence of an immediate and consistent response with the provisions of the INAIL Safety Management System, even if the final effect is it was partially nullified by an operational error (which was also promptly corrected) ";

- "the first incident was due to unidentified causes and occurred despite the system having passed, as illustrated, in-depth security checks as well as patch management and vulnerability assessment mechanisms and was protected [...] by appropriate authentication and authorization services , as well as IPS, WAF, Network Firewall, IPS host, antivirus and antimalware systems. As a measure aimed at avoiding further criticalities, the functionalities of the service in question were suspended. Following the analyzes carried out, failing to replicate the event that caused the violation in the laboratory and therefore define specific actions, also considering the low probability of occurrence, it was decided to put in place additional

checks on the tax code of the user whose information is displayed ";

- “the second accident occurred after the rehabilitation of the SVL functions, in any case protected by the technical and organizational security measures illustrated […], with the same unpredictability as the first accident. However, following the second incident, further extraordinary controls were introduced into the application, including a more granular tracking of the application actions in order to identify any new occurrences of the event, but also to immediately block the operation of the system should the error occur. to verify";

- "the third accident occurred due to a human error related to the release process in the operating environment, which resulted in the presence in operation of an incorrect version of the application. The production start-up process in INAIL environments has been codified and tested for years and provides for ex post checks of the transition of services to the operating environment. In the case in question, unfortunately, an operational error in the production release phase prevented the publication in operation of the version including the new additional controls useful for circumventing the anomaly ".

At the hearing, required pursuant to art. 166, paragraph 6, of the Code and held on XX, the Institute stated, in particular, that:

- "the Institute has adopted an information security management system and operates according to defined processes and procedures; in the last 3 years the Institute has obtained and maintained ISO 27001, ISO 9001 and ISO 20000 certifications ";

- "the central management of the digital organization deals with the development and management of the digital services of the Institute aimed at internal and external users, also identifying and adopting technical and organizational measures aimed at guaranteeing the security of information and the protection of personal data";

- "Each application service, before being released into production is subjected to a series of tests (performance, security, static quality of the code and accessibility) which are carried out by an organizational unit distinct from the one that deals with development; in addition, the release into operation is also carried out by a specific organizational unit; each activity is tracked through a ticketing system ";

- "in addition to the technical monitoring of services, the management of incidents and problems is entrusted to a specific organizational unit that adopts the ITIL methodology";

- "the story that is the subject of this proceeding begins in April 2019 when a user reports that, by accessing the SVL, he was able to view the files of two other subjects; in that circumstance, access to the SVL was promptly suspended and various tests were carried out, including performance tests, aimed at replicating the reported event; the source code was also analyzed,

without finding any application bugs; the most accredited hypothesis is that the incident may be connected to the management of the application sessions on the web servers that provide the service; after introducing a specific extraordinary application control (to verify that the files in the list displayed by the user referred to the authenticated user), the SVL was reactivated in autumn 2019 ";

- “subsequently, in November 2019, a new user reported that, by accessing the SVL, he was able to view practices related to six other subjects; in particular, the user, while viewing a list of files of his competence, by selecting them, accessed files containing data of other subjects; also on this occasion, access to the SVL was suspended in order to ascertain the causes of the accident; the SVL was reactivated in spring 2020 following the introduction of a new application control aimed at verifying that the data in the files accessed by the user referred to the authenticated user ";
- "in April 2020, the Institute received a new report from a user who was able to view the practices of two other subjects; on that occasion it was ascertained that the cause was not of a technical nature but of an organizational nature, as the software component that contained the application control introduced following the second report had not been released into operation due to a mistake; an audit was conducted that recommended the adoption of a dashboard for monitoring tickets that remain in the same state for too long, in order to prevent the occurrence of similar problems in the future ";
- "since that moment no anomaly has occurred, as can be seen from the logs produced by the SVL and from the fact that no reports have been received from users nor have any inefficiencies been reported on other channels (eg social networks)";
- "the protection of personal data is explicitly referred to also in the general security policy of the ISMS, the implementation of which is certified by the aforementioned ISO certifications";
- "the level of adequacy of the IT security measures adopted by the Institute is also certified by the rating that BitSight has attributed to the Institute, which is one of the highest in Italy";
- "the policies adopted by the Institute comply with the principles of safety in depth, the separation of roles and continuous improvement";
- "The Institute's information systems have always stood out for their efficiency and constant maintenance";
- "the Institute has adopted timely technical and organizational measures to limit the negative consequences for the interested parties involved and, in compliance with the principles of good faith and fairness, cooperated with the Authority during this proceeding";

- "the Institute believes that the treatments in question are attributable to the institutional functions of the Body and the display by each user of their personal data is not only lawful, but also necessary to allow consultation of the practices concerning them managed by 'Institute; the violations of the personal data in question are the result of accidental events, not characterized by willful misconduct or negligence ".

5. Outcome of the preliminary investigation

5.1. The legislation on the protection of personal data.

The personal data protection discipline provides that the processing of personal data by public entities can be carried out only if necessary "to fulfill a legal obligation to which the data controller is subject" or "for the execution of a task of public interest or related to the exercise of public authority vested in the data controller "(Article 6, paragraph 1, letters c) and e) of the Regulation).

The national legislation has also introduced more specific provisions to adapt the application of the rules of the Regulation, determining, with greater precision, specific requirements for processing and other measures aimed at guaranteeing lawful and correct processing (Article 6, par. 2, of the Regulation) and, in this context, has provided that the processing operations, and among these the "communication" and "dissemination" of personal data, are allowed only when provided for by a law or, in the cases provided for by law, regulation (Article 2-ter, paragraphs 1 and 3, of the Code).

With regard to the particular categories of personal data, including those relating to health (in relation to which a general prohibition of processing is envisaged, with the exception of the cases indicated in art.9, paragraph 2 of the Regulation and, in any case, a regime of greater guarantee with respect to other types of data, in particular, as a result of art. 9, par. 4, as well as art. 2-septies of the Code), the processing is permitted where "necessary for reasons of significant public interest on the basis of the law of the Union or of the Member States, which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to protect the fundamental rights and interests of the data subject "(Article 9 , paragraph 2, letter g), of the Regulation). The national legislator has defined the public interest as "relevant" for the processing "carried out by persons carrying out tasks of public interest or related to the exercise of public authority" in the matters indicated, albeit in a non-exhaustive manner, by art. 2-sexies of the Code, establishing that the relative treatments "are allowed if they are provided for by European Union law or, in the internal system, by legal provisions or, in the cases provided for by law, by regulations specifying the types of data that can be processed, the operations that can be carried

out and the reason of significant public interest, as well as the appropriate and specific measures to protect the fundamental rights and interests of the data subject ".

The data controller is required to comply with the principles of "lawfulness, correctness and transparency", "purpose limitation", "data minimization", "accuracy", "conservation limitation" and "integrity and confidentiality", as well as " empowerment "(Article 5 of the Regulation).

The owner must, in particular, ensure that the data are "processed in such a way as to guarantee adequate security of personal data, including the protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from loss, destruction or from accidental damage "(Article 5, par. 1, letter f), of the Regulations). In accordance with the aforementioned principle of "integrity and confidentiality", the data controller is required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, "taking into account the state of the art and the costs of implementation, as well as the nature, object, context and purposes of the processing, as well as the risk of varying probability and gravity for the rights and freedoms of individuals "; in assessing the adequate level of security, it is necessary to take into account, in particular, "the risks presented by the processing that derive in particular from [...] unauthorized disclosure or access, accidentally or illegally, to personal data transmitted, stored or otherwise processed "(Article 32 of the Regulation; see also recital 83).

5.2. The communication of personal data

At the outcome of the investigation, it emerged that - with the exception of the violation of 29 November 2019, which did not concern personal data of identifiable data subjects - in the context of personal data violations notified on 16 May 2019 and 24 April 2020, some users of the Service have had the opportunity to view personal data, also relating to health as they relate to accidents or occupational diseases, of other users (in particular: name, surname, type of practice - e.g. occupational disease or accident -, information on status and progress of the practice).

This has resulted in unauthorized access to personal data of third parties (different users), including those relating to health (Article 4, point 10), of the Regulation in the context of treatments attributable to the performance of the Institute's public interest tasks.) which configure communications of personal data, in violation of articles 5, par. 1, lett. a), 6, par. 1, lett. e), and 9, par. 2, lett. g), of the Regulations, as well as of articles 2-ter and 2-sexies of the Code (in the text prior to the amendments made by Legislative Decree No. 139 of 8 October 2021, applicable to the present case).

5.3. The security of the processing.

During the investigation it emerged that, as regards the violations of personal data notified on May 16, 2019 and April 24, 2020, the malfunction was attributable, respectively, to an unspecified "configuration of the software and middleware infrastructures" and to a "process error that led to the presence in operation of the wrong version of the application".

In this regard, it should be noted that the data controller is required to adopt adequate technical and organizational measures to ensure the confidentiality of the data processed on a permanent basis, as well as the integrity of the processing systems and services and that, in any case, he must adopt procedures "to test, verify and regularly evaluate the effectiveness of technical and organizational measures in order to guarantee the security of processing" (see Article 32, paragraph 1, letter b) and d), of the Regulation).

During the investigation, the Institute has documented that it has adopted an information security management system and that it operates according to processes and procedures, based on the ITIL V3 framework, which provide, among other things, that each service, before being released into operation, it is subjected to a series of checks (performance, safety, static quality of the code and accessibility) carried out by an organizational unit separate from the one that deals with development activities.

However, this did not prevent the occurrence of the security incidents underlying the violations in question and did not allow, in the first two cases, to identify the causes.

Moreover, with reference to the third security incident, as documented and confirmed by the owner himself, the violation was instead determined by a "human error" occurred in the process of release in the operating environment, which is, however, attributable to the sphere of responsibility of the owner.

For these reasons, it is believed that, at the time the personal data breaches notified on May 16, 2019 and April 24, 2020 took place, the Institute had not adopted appropriate technical and organizational measures to guarantee an adequate level of security for risks presented by the processing, thus determining the premises of the violations of personal data referred to above, in violation of articles 5, par. 1, lett. f) and 32 of the Regulations.

6. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the data controller during the investigation □ the truthfulness of which one may be called to respond pursuant to art. 168 of the Code □, although worthy of consideration, do not allow to overcome the findings notified by the Office with the act of initiation of the procedure and are insufficient to allow

the dismissal of this proceeding, since none of the cases provided for by the 'art. 11 of the Guarantor Regulation n. 1/2019.

Therefore, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by the Institute is noted, which led to unauthorized access by subjects other than those concerned to personal data, including those relating to health. , of other users, in a manner that does not comply with the principles of "lawfulness, correctness and transparency" and "integrity and confidentiality", in the absence of a suitable regulatory requirement and in the absence of technical and organizational measures suitable to guarantee an adequate level of security to the risk presented by the treatment, and, therefore, in violation of art. 5, par. 1, lett. a) and f), 6, par. 1, lett. e), 9, par. 2, lett. g), and 32 of the Regulations, as well as 2-ter and 2-sexies of the Code, in the text prior to the amendments made by the Legislative Decree. 8 October 2021, n. 139, applicable to the present case.

The violation of the aforementioned provisions makes the administrative sanction provided for by art. 83, par. 5, of the Regulation, pursuant to art. 58, par. 2, lett. i), and 83, par. 3, of the same Regulation, as also referred to by art. 166, paragraph 2, of the Code.

In this context, considering, in any case, that the conduct has exhausted its effects, the conditions for the adoption of further corrective measures pursuant to art. 58, par. 2, of the Regulation.

7. Adoption of the injunction order for the application of the pecuniary administrative sanction and ancillary sanctions (articles 58, par. 2, lett. I and 83 of the Regulation; art. 166, paragraph 7, of the Code).

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

In this regard, taking into account art. 83, par. 3, of the Regulations, in this case the violation of the aforementioned provisions is subject to the application of the pecuniary administrative sanction provided for by art. 83, par. 5, of the Regulations, as also referred to by art. 166, paragraph 2, of the Code

The aforementioned administrative fine imposed, depending on the circumstances of each individual case, must be determined

in the amount taking into account the elements provided for by art. 83, par. 2, of the Regulation.

In relation to the aforementioned elements, it was considered that the security incidents in question - albeit isolated and involving a small number of interested parties - are attributable to the sphere of responsibility of the Institute whose relevant institutional competences - including compulsory insurance against accidents at work and occupational diseases - require a high degree of responsibility (so-called accountability), in order to guarantee the safety of the treatment which also concerns information related to the health of a large number of interested parties, often vulnerable, given the subjects to whom the services offered are addressed.

On the other hand, it was taken into consideration that the violations of personal data concerned a limited number of data subjects (less than ten) and that, at least in one case, the incident was caused by "human error"; that the Institute promptly notified the aforementioned personal data violations to the Authority and promptly informed the interested parties involved in the violations, in accordance with Articles 33 and 34 of the Regulation, finally adopting measures deemed adequate to remedy the violations and mitigate their possible negative effects on the interested parties. The Institute also provided, also with the help of its Data Protection Officer, a particular collaboration during the investigation, taking steps to adopt technical and organizational measures aimed at conforming the treatments in progress to the regulations on the protection of personal data, in compliance with the principle of accountability. Finally, there are no previous relevant violations committed by the data controller or previous provisions pursuant to art. 58 of the Regulation.

Due to the aforementioned elements, assessed as a whole, it is believed to determine the amount of the pecuniary sanction in the amount of 50,000 (fifty thousand) euros for the violation of Articles 5, par. 1, lett. a) and f), 6, par. 1, lett. e), 9, par. 2, lett. g), and 32 of the Regulations, as well as 2-ter and 2-sexies of the Code, as an administrative pecuniary sanction, pursuant to art. 83, paragraph 1, of the Regulation, effective, proportionate and dissuasive.

Taking into account the nature of the data processed and the relevance of the services offered by the Institute on the national territory, it is also believed that the ancillary sanction of the publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Guarantor Regulation n. 1/2019.

Finally, it is believed that the conditions set out in art. 17 of Regulation no. 1/2019.

WHEREAS, THE GUARANTOR

pursuant to art. 57, par. 1, lett. a), of the Regulations, declares illegal the conduct of the Institute, described in the terms set out

in the motivation, consisting in the violation of Articles 5, par. 1, lett. a) and f), 6, par. 1, lett. e), 9, par. 2, lett. g), and 32 of the Regulation, as well as 2-ter and 2-sexies of the Code, in the terms set out in the motivation;

ORDER

pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, to the National Institute of Accident Insurance at Work, in the person of the pro-tempore legal representative, with registered office in Via IV Novembre, 144 - 00198 Rome (RM), Tax Code 01165400589, to pay the sum of € 50,000 (fifty thousand) as a pecuniary administrative sanction for the violations indicated in the motivation. It is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the sanction imposed;

INJUNCES

to the aforementioned National Insurance Institute for Accidents at Work, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of € 50,000 (fifty thousand) according to the methods indicated in the annex, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the l. n. 689/1981.

HAS

- the publication of this provision on the website of the Guarantor pursuant to art. 166, paragraph 7, of the Code (see Article 16 of the Guarantor Regulation No. 1/2019);
- the annotation of this provision in the internal register of the Authority, provided for by art. 57, par. 1, lett. u), of the Regulations, violations and measures adopted in compliance with art. 58, par. 2, of the Regulation (see article 17 of Regulation no. 1/2019).

Pursuant to art. 78 of the Regulation, 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision, it is possible to appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the applicant resides abroad.

Rome, April 28, 2022

THE VICE-PRESIDENT

Cerrina Feroni

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei

* The provision was challenged