[doc. web n. 9751194]

Injunction order against the National Institute of Statistics - 10 February 2022

Record of measures

n. 46 of 10 February 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, Prof. Ginevra Cerrina Feroni, vice president, Avv. Guido Scorza, member, and the cons. Fabio Mattei, general secretary;

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

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

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

GIVEN the documentation in the deeds;

HAVING REGARD to the observations made by the Secretary General pursuant to art. 15 of the Guarantor Regulation n. 1/2000;

Speaker prof. Pasquale Stanzione;

WHEREAS

1. The breach of personal data

The National Statistical Institute (Istat), with an act of 8 November 2020 notified a violation of personal data, pursuant to art. 33 of the Regulation, announcing that it has also prepared the complaint for the Postal Police (then transmitted in deeds and

dated 9 November 2020), and with subsequent notes of 9 November 2020 (prot.n.2263370), 20 November 2020 (prot. n.2301044), 28 November 2020, (prot.n.2366761), 1 December 2020 (prot.n.2411492), 3 December 2020, (prot. of the art. 33, par. 4 of the Regulations, also in response to specific requests for information from the Guarantor's Office (notes of 16 November 2020, prot. No. 43293 and of 26 November 2020, prot. 45049).

The violation consisted of a cyber attack that led to the exfiltration of some information and the potential unauthorized access by third parties to the information, including authentication credentials contained, respectively, in the "COEWEB" and "INDATA" portals reachable at following URLs https://www.COEWEB.istat.it and https://INDATA.istat.it/pdc.

1.1 The violation of the COEWEB portal

In the notification, the Institute stated that "the site www.COEWEB.istat.it, used for the dissemination of statistics on foreign trade", was the subject of a violation, caused by an intentional external action, made publishes on November 5, 2020, which the owner was aware of through reporting by the CSIRT-ITA (Computer Security Incident Response Team - Italy) and by the CERT-GARR (Computer Emergency Response Team of GARR - Research Network Extension Management - or the community of education and research) without being able to trace the time of the attack.

In particular, Istat stated that "the violation was published by anonymous Italy at the following link: https: // ...". According to what was known at the time of the notification, "only the names of the DBs were disclosed, but the vulnerability analysis does not exclude the possibility that further data have been exfiltrated (user data and public macro-data for the diffusion of foreign trade) ".

The violation would therefore have caused the potential loss of confidentiality of personal, contact, access and identification data referring to approximately 27,000 interested parties, including employees, consultants, users also from other countries belonging and not to the European Economic Area. According to the documents, "the data subject to the violation include name, surname and address where present (non-mandatory fields), user's e-mail, username and password of the 'COEWEB.istat.it' application".

In describing the violation, it was stated that:

- “the violation was made through a sql injection attack, exploiting an application vulnerability. The sql injection attack is used on applications that manage data through relational databases using the SQL language. It is an attack that is activated due to vulnerabilities in the application logic. The vulnerability allowed access to the data in the database ”.

In this regard, Istat specified that it had activated further investigations in order to verify the possible dissemination of the exfiltrated data and that "access to 'COEWEB.istat.it' was immediately blocked and will be restored after resolving the identified vulnerabilities "and that" all users of the system have been disabled, users will have to register again at the next access ".

With reference to the possible consequences of the attack, it was highlighted, in particular, that:

- "the authentication credentials (username and local password of the system) are not used to access further data contained in the 'COEWEB.istat.it' system other than those that can be accessed without registering, taking into account the fact that the COEWEB are aggregated and aimed at dissemination to the public. By registering, a user profile is created in which the requests made by the user are saved in order to propose them again later with the updated data. It should also be noted that part of the email addresses are associated with offices and organizations and not directly with individuals ";
- “the IT incident involved a web server XX dedicated to the application www.COEWEB.istat.it and two database schemes XX containing the data for the dissemination and the authentication data of the users of the system. (...) ";

with reference to the measures implemented at the time of the violation, "the technical and organizational security measures adopted were deemed adequate in relation to the type of data processed intended for public disclosure:

- 1) authentication to the system via username and password (for the 'authenticated' part);
- 2) authentication to the server with "root" or "admin" administrator privileges, takes place after prior communication to the manager of the ITA service of the DCIT by means of an e-mail message, containing all the connection data and the reasons for which it is it is necessary to access with non-personal users ".

Following the violation and to reduce its effects, Istat stated that "the site was immediately made unavailable and all the users of the system were disabled; users will need to re-register at the next system restore login. The security team is monitoring and analyzing vulnerabilities which also makes use of the support of "ethical hackers" in order to identify any possible vulnerability and update the software with the application of appropriate security patches that among other things, eliminate any possible sql injection attack such as the one that took place. When the site is restored, an information message will appear for users in which the incident will be highlighted and new security requirements will be provided for the creation of new credentials, as a precaution, despite the fact that it is a system of public data consultation only. and aggregates ".

To prevent similar future violations, Istat stated that [OMISSIS], that "the redesign of the COEWEB system is being evaluated"

and that "the software already in use is continuously and promptly analyzed to identify any new vulnerabilities".

Finally, Istat declared that on 9 November it would communicate the violation to the interested parties by publishing a specific message on a special courtesy page.

For the reasons set out above, the data controller has estimated the severity of the violation as "high".

In highlighting the causes that, also from a technical and organizational point of view, determined the violation in question, Istat, with a note dated November 20, 2020, stated in general that "due to errors in the software development process (...) an unknown code vulnerability occurred at the application level that allowed an attack from the outside ".

With specific reference to the COEWEB portal, it was subsequently declared that "the attack was made possible due to the presence of a" lack of input validation "vulnerability, (...)", that "registered users (registration e-mail number) are 31,080, of which 5,659 have the name, surname and address fields empty (i.e. no personal data is present). A further 200 records do not contain personal data, but references to offices, secretariats of public bodies and companies "and that" A percentage of registered users does not contain personal data but only references to offices, secretariats of public bodies and more often companies. Before the accident, the system did not provide for a mandatory password expiration ".

With reference to the security of the access passwords to the portal in question, it was specified that "in evaluating the technical and organizational security measures, the nature of the data hosted on the COEWEB system, or public statistical macro data relating to trade, was essentially taken into account with foreign countries, therefore not critical in terms of confidentiality. The registration of users was provided to allow you to store the so-called "Query" to the system, with a view to providing a better quality service ".

It was then shown that “in the version prior to the violation, the portal provided for the password stored in clear text, the maximum length of 8 characters and the obligation of only alphanumeric characters. It should be noted that these settings represent an exception with respect to the standard security policies of the Institute (...), and that the credentials for accessing COEWEB, (...), are only used to allow users to retrieve each session query and useful information previously saved and not because COEWEB requires authentication for restricted access services. Following the violation, the credentials have undergone a reset, so when the system is restored, users will be forced to register again. [OMISSIS]

1.2. The violation of the INDATA portal

In the notification, the Institute stated that "on November 5, 2020" the violation was also made public, known through the

CSIRT-ITA and CERT-GARR report, without being able to identify the moment of the attack, which concerned "the INDATA.istat.it/pdc site used for the data collection of the statistical survey of building permits".

In particular, it was stated that "the violation was published by anonymous Italy at the following link: https: // ...".

According to what was known at the time of the notification, "only the names of the DBs were disclosed but the analysis of the vulnerability does not exclude the possibility that further data have been exfiltrated (...)".

Even this violation would therefore have caused the loss of confidentiality of personal, contact, access and identification data referring to approximately 108,000 interested parties including employees, consultants and users.

The potentially violated data concern “name, surname and e-mail address of the authorized technician; non-personal cadastral data available to the public (relating to the object of the building permit); username and password of the applications 'INDATA.istat.it/pdc and INDATA.istat.i / pdcom' ". It was specified that "the system provides for two types of users:

- Municipality user (about 8000 whose format is XX) with an associated email address of the contact person identified by the Municipality;

- the users of the Technicians (about 100,000; each technician, if he works on several municipalities, has a user for each municipality, XX format) ".

In describing the violation, it was stated that it was carried out using the same sql injection attack operated on the COEWEB application and that "the IT incident involved a web server XX dedicated to the" INDATA.istat.it/ application. pdc and INDATA.istat.it/pdcom "and various database schemes XX containing the data of the survey of building permits and the authentication data of the users of the system".

With regard to the consequences of the violation, the Institute represented, in particular, that:

"The data could be disclosed, but it must be taken into account that:

- access to 'INDATA.istat.it/pdc and INDATA.istat.it/pdcom' was immediately blocked;

- passwords encrypted using the system's native functions;

- all system users have been disabled, users will have to change their password at the next access after the system is updated and reactivated ".

The measures to ensure the security of the processing, in place at the time of the violation, described in the notification deed are substantially similar to those reported in reference to the COEWEB portal.

In relation to the measures adopted to reduce the effects of the violation, in addition to what has already been represented for the COEWEB portal, it was declared, in particular, that "the complete migration of the compromised system has been prepared on a system that is intact with the basic software, the database server and the web server updated to the latest releases and compatible with the host application ".

Istat also stated that on 9 November it would communicate the violation to the interested parties by publishing a specific message on a special courtesy page, having estimated the seriousness of the violation as "high".

With a note dated 20 November 2020, with specific reference to the INDATA portal, it was stated that "from an analysis of the access logs to the" INDATA.istat.it/pdc "application in the month prior to the accident, a series of attempts emerged attack in ways compatible with the incident. Among these attempts, a series of requests was identified, on 29/10/2020, which presumably allowed the threat agent to access the data managed by the application and are therefore attributable to the incident to which the system".

In this context, more precise indications were also provided in relation to the interested parties whose data were violated, specifying, in particular that "the total registered users are 105,448, divided into 7,119 operators of the municipality and 98,329 technicians (surveyors, architects)" and that “the personal data stored are user, password, name, surname, e-mail. The total registered users are 105,448, divided into 7,179 operators of the municipality and 98,269 technicians (surveyors, architects), divided in terms of time [...]. Please note that the technician must have a user for each municipality in which he works. Before the accident, the system did not provide for a mandatory password expiration ".

In providing the clarifications required regarding the security measures related to passwords for access to the INDATA portal, it was stated that:

- "In the version prior to the violation, the portal provided for the following authentication procedure:

to register, the user was given an initial password, consisting of six alphanumeric characters preceded by the suffix "pdc", with which it was possible to activate the access credentials, creating a personal password, consisting of a minimum of 8 alphanumeric characters, encrypted with md5 algorithm. In the event that the user had lost the initial password, in order to register, he would necessarily have to contact customer support to get the same initial password back. The user logged in to the application through the access page, in which the credentials of the user code and personal password were verified. There was no expiration of the personal password. In case of loss of the personal access password, it was necessary to reset it using

the password reset page, for which it was necessary to have the initial password provided during registration. In the event that the user had to reset the password since he no longer had the initial password, he would have to contact the assistance to regain the same initial password provided during registration. The user could freely proceed to change his personal password, at any time, through the password change page, and having his own user code and personal password, creating a new personal password, consisting of a minimum of 8 alphanumeric characters. and encrypted with md5 algorithm ".

- "The new authentication procedure is as follows:

[OMISSIS]

- [OMISSIS]

It was therefore specified that, following the restoration of the portal [OMISSIS]

In indicating the further initiatives adopted, or intended to be adopted, in order to better identify the extent of the violation of personal data and the related risks for the rights and freedoms of the data subjects with regard to the INDATA portal - also in reference to the IST survey- 00088 referred to in PSN 2020-2022 (which, from the documentation on file, seemed to refer to the portal in question) -, it was specified that "(...), INDATA represents a gateway to different data collection sites, each of which it is characterized by applications and a dedicated database. The violation occurred on a so-called site "Satellite" of the INDATA portal, or INDATA / PDC, which is physically and logically separated from INDATA and the other data collection systems. The application targeted by the attack, INDATA.istat.it/pdc, is attested on a dedicated server on which no other applications reside and for which it is expected to be discontinued, as already described above, by migrating the application to new environments updated. In line with what has just been specified, with reference to the application that manages the IST00088 survey referred to in PSN 2020-2022, it is reiterated that this is attested on another server, or in an environment completely separate from the one subject to attack, and that the reference a INDATA in the PSN form of the IST00088 survey represents in a summary and concise way the circumstance that the data are collected through an acquisition portal. In other words, the servers and databases of the two applications that manage INDATA / PDC and the IST00088 survey have no element in common ".

1.3. Communication to interested parties and other elements

With a note dated 9 November 2020 it was specified that, in accordance with the indications of the postal police "it was decided to formulate a simple technical communication of unavailability of access to the INDATA and COEWEB sites, and to

communicate to users, via e-mail (...) ", subsequently, the Institute sent a complete communication to the interested parties in order to minimize the potential risk of incurring" credential stuffing "or" phishing "(notes of 20 and 28 November 2020).

In relation to both sites, Istat also specified that "these services were developed at the beginning of the 2000s and that, although improvements have been made over time, the nature and obsolescence of the code did not allow the implementation effective patching and updating policies. Therefore, depending on the nature of the services provided and the data present on both systems, considered low risk in terms of privacy, (...), as well as on the basis of cost and benefit assessments, the strategy adopted by the Institute provided for the segregation of the systems in question from the rest of the Istat information system ".

It was in fact specified that the COEWEB portal hosts "public statistical macro data, relating to foreign trade, therefore not critical in terms of confidentiality" while the INDATA portal hosts "non-personal cadastral data available to those who are entitled to access it ".

Istat stated, however, that "the migration of the same to safer environments is planned, with relative rewriting of the application code, in line with the technological and safety standards in use in the Institute. It is estimated that the migration activity will be completed by the first half of 2021 "and that, for both portals, the inclusion in a systematic software analysis process (ALM) aimed at identifying and promptly remedying any vulnerabilities has been envisaged .

With a note dated 1 December 2020, Istat finally clarified that the different password policies adopted for the portals subject to violation were motivated by the different types of data processed compared to the other databases of the Institute and declared that it had, following the security incident that has occurred, they have been adapted to the standards of the Institute as illustrated above.

The Institute also confirmed that "it had remedied the aforementioned vulnerability on the INDATA / PDC portal, currently online" and that it had "performed specific vulnerability tests to test its effectiveness before precisely the new availability for the system user" and that "The two applications COEWEB and INDATA / PDC are part of the standard process of the Institute for the management of ALM applications (Application Lifecycle Management) and in the cycles of periodic vulnerability assessment". With reference to the COEWEB portal, it was stated that it "will be redesigned by the end of June 2021, ensuring, in the meantime, the patching of the version that will be deprecated, even in the intermediate release which will take place by the end of 2020".

With a note dated 3 December 2020, following further in-depth checks, Istat declared, with reference to the INDATA portal, that "the breach of the system is configured as a security incident, but not as a breach of personal data" and that "the incident on COEWEB is a security incident and the risk that personal data have been exfiltrated is very low".

In particular, Istat declared that it had "(...) analyzed the logs of the INDATA / PDC application containing the details of the individual queries performed (" queries "log file). The “queries” file reports all the instructions (sql commands) launched towards the database. This file shows, in the time between 16.30 and 17.44 on 29 October 2020, a blind SQL injection attack, the purpose of which is to try to understand the characteristics of the site attacked through its vulnerabilities and then retrieve information. The log analysis made it possible to verify that, during the attack, all and only the exfiltrated information consisted of the data schema of the PDC Data Base and the name of all the tables contained in the aforementioned schema, used by the application. There is therefore no trace of further data exfiltration, including the personal data of the users certified on the system. After October 29 and until the closing date of the site, there are no further attacks. It can therefore be said that this incident does not constitute a breach of personal data ”.

With reference to the COEWEB portal, Istat declared that it had "analyzed the COEWEB application logs produced by the activities operated on the IIS web server, also containing the calls to the aforementioned web server, which direct queries to the underlying DB XX (it is the DB which also contains personal data). These calls are classified according to the two types "GET" and "POST". For all the calls it was possible to identify the IP address of origin and the type (GET / POST). For GET calls it was possible to identify exactly the query sent to the DB. An analysis of the log file highlights a blind SQL injection attack, the purpose of which is to try to understand the characteristics of the site attacked through its vulnerabilities and then retrieve information. The IP of origin of the attack and the exact duration of the attack were identified, which began on 29 October 2020 at 12.11 and ended the same day at 16.22. A key element of analysis is the fact that the blind SQL injection attack is time consuming, that is, it requires time and queries to steal the information of interest ".

A "chronological reconstruction of the action of the attacking program" was also provided on the basis of which:

- "From 12.11 to 12.30 the attacker, through specific calls to all COEWEB pages, tries to find a vulnerability point. Therefore, this period of time can, to all intents and purposes, be considered an exploratory phase on the part of the attacker or it can be said with certainty that no type of information is exfiltrated.
- From 12.31 to 12.57 the attacker begins to check the possibility of an sql injection attack and confirms that he can exploit this

vulnerability at 12.57. Even at this stage it can be said with certainty that no type of information is exfiltrated.

- From 12.58 to 16.07 the attacker exploits the sql injection vulnerability to obtain information relating to the structure of the database and obtains all the data schemes present on the DB (which are exactly those published by anonymus), including the DB “owner” data schema. Even at this stage, no personal data is exfiltrated.

Taking into account that the attacking program has obtained only a first information relating to the database schema (and therefore neither the names of the tables, nor the data contained in them), from 16.08 to 16.22 the last phase of the attack, they infer about 370 POST calls, and one can therefore only speculate what information the attacker could potentially obtain.

We place ourselves in the worst case scenario, in which the attacker obtains as much information as possible with the 370 calls detected and all considered effective for the purpose.

Since the attacker has identified the owner of the DB, he needs at least 16 queries to obtain the names of the 16 tables that make up the DB, a further 16 queries to obtain the number of fields that make up each table, 214 total queries to obtain the names of all the fields that make up the tables, 16 queries to obtain information on the number of records per table.

Adding up all these queries (which are considered to be successful in a highly unlikely scenario) the attacker made 262 queries. He then has about 110 additional queries left.

Considering that of the 16 tables that make up the DB only table 8 and table 14 contain personal data (userid of the COEWEB site, password, email), being able to reach this information with an automatic program, which analyzes sequentially the tables, from the first to the sixteenth, is almost impossible because the number of queries left is about 110 while the number of records of the first table is over 1 million. So the attacker could not even exfiltrate the (non-personal) information contained in the first table, because he would have needed at least 1 million queries.

The Institute reiterates that this scenario is extremely unlikely due to the type of attack and the structure of the tables in question.

After October 29 and until the closing date of the site, there are no further attacks.

It can therefore reasonably be said that the attack limited itself to demonstrating the vulnerability of the site and what Anonymous was exposed to is exactly what is obtained from the queries analyzed ".

In light of these considerations, the Institute has reassessed the seriousness of the violation and the related risks in terms of improvement.

2. The investigation activity

In relation to what was notified and the additional elements provided, the Office, with deed prot. n. 0045434, of 9 September 2021, notified Istat, pursuant to art. 166, paragraph 5 of the Code, the initiation of the procedure for the adoption of the measures, referred to in Article 58, paragraph 2 of the Authority (art. 166, paragraphs 6 and 7, of the Code; as well as art. 18, paragraph 1, of the law n. 689 of 24 / I / 1981).

With the aforementioned deed, the Office considered that the Institute, at the time the attacks described above occurred, in the context of the INDATA and COEWEB portals, processed the personal data of users authorized to access them, in the absence of technical measures and organizational structures capable of guaranteeing an adequate level of security for the risks presented by the processing, in violation of the principle of integrity and confidentiality, pursuant to art. 5, par. 1, lett. f) of the Regulations and with technical and organizational measures that are not suitable for ensuring an adequate level of security on a permanent basis in violation of art. 32 of the Regulation.

With a note dated 6 October 2021 (prot. No. 2628947), the Institute sent its defense briefs, without making a specific request for a hearing.

In this context, as a priority and in general terms, the Institute represented the ability to operate "in compliance with the principles of protection of personal data", which "has been involved for years in the definition and adoption of technical security measures and organizational, with a view to their adequacy in accordance with current legislation and industry best practices, with the aim of increasing the security of the systems and processes supporting the processing of personal data, with a risk-based approach, in consistent with the Agid guidelines "and to have" undertaken a path aimed at ensuring the adoption of adequate protection measures for its systems. In particular, since 2017, Istat has intended to continuously strengthen and improve its IT and information infrastructure by adhering to the ISO / IEC27001 reference standard "and to" extend the scope of certification [ISO / IEC 27001: 2013] to the entire technological infrastructure to support statistical production […] by 2022 ".

Istat highlighted that at the time of the attack, the INDATA / PDC and COEWEB systems were "rigidly" segregated "from the other systems of the Institute through the adoption of local access credentials that did not allow, if violated, to access other servers ".

The Institute specified that, taking into account the type and quantity of data managed, which make it a unique reality in the PPAA scenario, the path for adopting or strengthening the necessary technical and organizational measures is determined by

giving priority "in relation to the underlying risk to the processing of personal data related to specific systems ", and also conditioned on the availability of economic resources. In this regard, it was reported that “Istat's average expenditure for IT security in the last 5 years is equal to 6.9% of total IT expenditure”.

Having said this, with reference to the violations that occurred, it was reiterated that on the INDATA portal the violation "was re-qualified as a security incident and not as a data breach, as the only information exfiltrated was the database schema relating to INDATA / PDC and the name of the tables contained therein, without any personal data "while on the COEWEB portal the violation was re-qualified as of" low "severity.

It was also specified that "both sites, INDATA / PDC and COEWEB, allowed the registration of users for the sole purpose of facilitating the same in saving searches related to the data published by Istat and contained within the two databases. The processing of personal data, therefore, concerned the storage of a limited number of contact details of the users who provided the data only for the purpose of carrying out their professional activity and accessing the aforementioned portals ".

In underlining the absence of intentionality with respect to the events in question, the Institute reiterated how they were caused by an intentional external action and how the Authority ordered the immediate blocking of access to the aforementioned portals and followed up the migration of the same "on an updated infrastructure and in line with the standard process of the Institute for the management of ALM applications".

In relation to the measures implemented to prevent the recurrence of similar future events, Istat stated that:

[OMISSIS]

[OMISSIS]

It was also pointed out that "more than 10 months after the IT attack that occurred, the Institute received no reports from interested parties about any damage suffered attributable to this event" and that "it is possible to exclude from the scope of the violation the data referred to in Articles 9 and 10 of the Regulations ".

Finally, the Institute highlighted the high degree of cooperation with the Authority and that it promptly notified the event to the Guarantor, addressing it with extreme care and choosing, in a prudent way pending the determination of the actual risk level, to take "In the worst-case scenario" and to communicate the violation to the interested parties, "in order to make them aware of the hypothetical risks deriving from a scenario of compromising the confidentiality of their login credentials to the portals".

3. Outcome of the preliminary investigation

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

on the basis of the principle of integrity and confidentiality (Article 5, paragraph 1, letter f) of the Regulation), personal data are processed in such a way as to guarantee adequate security of personal data, including protection, by means of technical and adequate organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage; in the processing of personal data, the owner must put in place adequate technical and organizational measures to guarantee a level of security appropriate to the risk, which include, among others, the ability to ensure the confidentiality of data on a permanent basis and a procedure for testing, regularly verify and evaluate the effectiveness of technical and organizational measures in order to guarantee the security of processing (Article 32 of the Regulation).

Having said this, taking into account the statements collected during the investigation - and considering that, unless the fact constitutes a more serious crime, whoever, in a proceeding before the Guarantor, falsely declares or certifies information or circumstances or produces false documents or documents it responds pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor" -, the elements provided by the data controller in the defense briefs do not allow to overcome the findings notified by the Office with the act of initiation of the procedure, however, as none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

For these reasons, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by the National Statistical Institute in violation of the principle of integrity and confidentiality (5, paragraph 1, letter f), of the Regulation is noted.) due to the absence of technical and organizational measures suitable for guaranteeing an adequate level of security for the risks presented by the processing, at the time the attacks described above occurred, within the INDATA and COEWEB portals (Article 32 of the Regulation). In fact, despite no data has been exfiltrated from the INDATA portal and despite the violation of the COEWEB portal has been redeveloped as of "low" severity, it is established that Istat, as data controller and holder of large databases, exposed for their very nature with a high probability of attack, did not have, also taking into account the technological state of the art, suitable technical measures to guarantee on a permanent basis the security and confidentiality of the data processed within the two aforementioned portals.

4. 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 violation of articles 5, par. 1, lett. f) and 32 of the Regulations, caused by the conduct of the Institute is subject to the application of a pecuniary administrative sanction pursuant to art. 83, par. 4, a) and par. 5, lett. a) of the Regulations.

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

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

from the results of the documents, the episode appears to have been completely isolated and determined by an accidental external action;

the violation, not preceded by similar events, lasted for a short period of time;

the risk that there has been a violation of the confidentiality of the personal data of the users of the COEWEB application has been calculated, on the basis of specific quantitative parameters, as extremely low if not residual and that in any case such information does not concern the particular categories of data or data relating to criminal convictions and offenses, referred to in articles 9 and 10 of the Regulations;

it was not possible for the Institute to define the number of interested parties involved in the violation;

the owner has notified the event to the Authority without undue delay, pursuant to art. 33 of the Regulation;

the owner communicated the violation to the interested parties, pursuant to art. 34 of the Regulation;

the interested parties have not submitted complaints to the data controller or suffered damage from the event that occurred;

the owner subsequently provided for the implementation of new and specific technical and organizational measures aimed at preventing the recurrence of similar future events;

the event that occurred is attributable to the slight negligence of the owner, who has adopted technical and organizational measures that are not adequate to the state of the art to ensure a level of protection and safety, including application,

adequate to the risk of the processing. In particular, consider: i) that storage through the use of state-of-the-art cryptographic techniques is one of the measures commonly adopted to protect the passwords of users of an online service, while Istat retained, with respect to the aforementioned services , passwords in clear text or through an algorithm that is not robust at the technological state of the art; ii) the obsolescence of the systems; iii) the presence of specific vulnerabilities within the portal code;

the conduct was caused by Istat's need to give priority, due to the large number of databases managed, to the implementation of the necessary technical and organizational measures on the systems that expose the interested parties to greater risks in terms of severity and chance;

the owner proved to be cooperative throughout the preliminary and procedural phase;

no complaints or reports have been received to the Guarantor on the incident.

Due to the aforementioned elements, assessed as a whole, it is believed to determine the amount of the pecuniary sanction provided for by art. 83, par. 5, lett. a) of the Regulations, to the extent of € 6,000.00 (six thousand) for the violation of Articles 5, par. 1, lett. f) and 32 of the Regulations as a pecuniary administrative sanction, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary sanction of the publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Guarantor Regulation n. 1/2019.

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

ALL OF THIS GIVEN THE GUARANTOR

pursuant to art. 57, par. l, lett. a) of the Regulations, declares the unlawfulness of the processing of personal data carried out by the National Institute of Statistics, with registered office in via Cesare Balbo, 16 - 00184 Rome, cf | 80111810588, for the violation of the principle of integrity and confidentiality, pursuant to art. 5, par. 1, lett. f) of the Regulations, and of art. 32 of the Regulation, due to the absence of technical and organizational measures suitable for guaranteeing on the INDATA and COEWEB portals an adequate level of security for the risks presented by the processing;

ORDER

at the National Institute of Statistics, with registered office in Via Cesare Balbo, 16 - 00184 Rome, cf | 80111810588, pursuant

to art. 58, par. 2, lett. i) and 83 of the Regulations, as well as art. 166 of the Code, to pay the sum of € 6,000 (six thousand) as a pecuniary administrative sanction for the violations indicated in the motivation;

INJUNCES

to the National Institute of Statistics to pay the sum of € 6,000 (six 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. In this regard, it is recalled that the offender has the right to settle the dispute by paying - again according to the methods indicated in the annex - of an amount equal to half of the sanction imposed, within 30 days from the date of notification of this provision, pursuant to art. 166, paragraph 8, of the Code (see also Article 10, paragraph 3, of Legislative Decree no. 150 of 1/9/2011);

HAS

pursuant to art. 166, paragraph 7, of the Code, the full publication of this provision on the website of the Guarantor and believes that the conditions set out in art. 17 of Regulation no. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

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

Rome, February 10, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Stanzione

THE SECRETARY GENERAL

Mattei