SEE ALSO NEWSLETTER OF 22 JUNE 2021

[doc. web n. 9669974]

Provision of May 13, 2021

Record of measures

n. 190 of May 13, 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, 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 4/4/2019, 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 on the organization and functioning of the office of the Guarantor for the protection of personal data, Doc. web n. 1098801;

Speaker prof. Pasquale Stanzione;

WHEREAS

1. The complaint.

With a complaint of the XXth, an employee of the Municipality of Bolzano (hereinafter "the complainant") complained about alleged violations of the personal data protection regulations with regard to the processing of data put in place by the Entity through the monitoring of network traffic and of the individual Internet accesses made by the interested party and, in general, by municipal employees.

In particular, the complainant complained that the Entity would have processed personal data relating to his Internet browsing, during working hours, and that he had received, on the 20th date, a notice of initiation of disciplinary proceedings (see note of the XX attached to the complaint), in which he was accused that "in the period from XX to XX, he was [...] connected [o] with the computer of the Municipality, for over 40 minutes on facebook and for over 3 hours on youtube, to follow non-institutional activities and who […] had consulted Internet pages not related to his work ”as resulting from the data traffic records of the Municipality of Bolzano (see reports attached to the complaint). These data would be used to formulate disciplinary findings, upon request of the Director of the Territory Management Office to the IT Services Office of the Entity (see Annexes nos. 2 and 3 to the complaint). Subsequently, the disciplinary proceedings would have been filed for reasons relating to the unreliability of the data collected (see annex. No. 8 to the complaint).

The complaint complained about the violation of the principles of lawfulness, correctness and minimization in the processing of the personal data of the employees of the Municipality, given that the Internet access registration system used by the Authority would allow to "control, trace, filter in a massive, constant and indiscriminate [...] the history of the websites visited and the browsing time for each site "(see complaint, p. 6), as well as the storage and conservation of such data associated with each employee for a long period of time. This would, therefore, have made it possible, by forwarding a specific request to the IT Services Office of the Entity, to verify the individual sites visited by the interested party, by extracting reports (see reports relating to the complainant, Annex 4 to the complaint), resulting in a “remote control unjustly damaging to freedom and dignity […] and prohibited by art. 4 of the l. 300 of 1970 "(see complaint p. 7).

The processing would have taken place in the absence of information to employees regarding possible controls on Internet access by the employer, specifying that "for this purpose the content of the trade union agreement of 25.10.2010 cannot be considered exhaustive unless absolutely no limits are indicated with reference to internet browsing or to what extent it is allowed to use the network for personal reasons and in which cases control can be triggered; then there is no information regarding the processing of the data acquired, the person responsible for such processing and its purpose "(see p. 7

complaint).

With the same complaint, the interested party also complained about the non-compliance with the principles of protection of personal data of the internal procedure for the use of the psychological assistance service made available to employees. From this point of view, it has been shown that the procedure provides for the compilation of the form called "Request for an extraordinary medical examination", to be sent to the company that performs the functions of competent doctor on behalf of the administration and to the "respective Department Manager of the employee" (see p. 9 complaint). In the specific case, the manager of the complainant would have signed "for acknowledgment" on XX the form presented by the person concerned to the competent doctor.

The complainant therefore asked the Guarantor to "verify the lawfulness of the processing" of data put in place by the Municipality, "to declare illegal the processing that violates the legislation and principles regarding the protection of perianal data, as well as the art., 4 l. 300/1970 "," declare the unusability of the information found in violation of the law and order the prohibition of further processing and retention of data "and" order the transmission of documents to the judicial authority for assessments of competence in relation to criminal offenses that it may deem to be configurable "(see p. 10 complaint).

2. The preliminary activity.

In response to the specific requests of the Office regarding the numerous profiles raised by the complaint, the Municipality sent the note of the XXth, with which the following was specified:

- the "decentralized trade union agreement for the use of the Internet / intranet and use of e-mail" of the twentieth states that "managers can ask the network administrator for targeted checks on internet access by the staff of the respective office / division ";

- of this agreement, "published on the intranet page of the home page of the Municipality of Bolzano", the complainant "was perfectly aware" (this would be proven by the documentation relating to the acknowledgment by the interested party on the matter, see Annex 1B and 2C to the cited note);

- "art. 10 of the Code of Conduct for employees, published on the intranet page of the home page of the Municipality of Bolzano, [...] expressly provides that [...] the use of all IT tools, whether software or hardware, made available to provision by the Administration is limited to work needs "and that" on the intranet page of the home page of the Municipality of Bolzano on the page that describes the methods of accessing the Internet-Mail service, it is highlighted in red and in bold that " sites visited

"(annex no. 4 cit. note);

- "the collection of logs by the municipality has the primary objective of recording user events for the purposes defined by the trade union agreement and, in particular, to generate evidence for the IT security of the Municipality network [...] which falls within in art. 6, lett. e) of the GDPR as aimed at preserving the municipal network in the execution of its tasks of public interest [...] "; moreover, "the activity of logging and monitoring is strongly recommended to guarantee IT security (eg ISO 27001 and 27002 and the Enisa measures of the Manual on security in the processing of personal data [...]" (see p. 6 cit. Note);

- with regard to the processing methods, it was declared that “the trace is updated daily by overwriting [the] on the 30th day [... and] therefore it is deleted. Therefore, only the traces of the last 30 days are kept as required by the trade union agreement ";

- moreover, "the tracking of data, as a security measure, allows the user to see anomalies on his accesses, with the obligation in this case to immediately communicate them to the network administrator"; "The improper use of accesses, reported by a sector manager, involves, if required, the disabling of access and the activation of any disciplinary proceedings against the defaulting party"; "Executives, who have an obligation to monitor collaborators [...] can ask the network administrator for targeted checks on the staff of their respective office";

- the Municipality felt that it had fulfilled its obligation to inform employees by means of the following documents: the general information (made prior to the entry into force of the Regulations and the subsequent one, "published on the institutional website"), the trade union agreement cited, the form that each employee must sign when requesting access to the Internet (based on two different levels of access for the use of the Internet by employees established by the administration: the so-called "extended" and the so-called "limited "); the code of conduct and the internal circulars of the Personnel Office (see p. 7 cit. note); following the request for information, the Municipality has undertaken, for the future, to draw up a single "disclosure dedicated to the processing which for organizational needs and / or IT security measures entail the tracking of employee activities" and, in general "To unify the information concerning the personal data of employees or collaborators, information available today on the internet under the individual organizational structures on the basis of specific skills" (see p. 11, cit. Note);

- the data protection officer of the Entity expressed himself "on the risk analysis carried out by the internal managers on the treatments surveyed by competence, validating them or making observations relating to any improvement measures to be taken"; this analysis "did not reveal any high risk to the rights and freedoms of individuals and therefore pursuant to art. 35 of

the GDPR, no impact assessment was required "(see p. 10, cit. Note);

- the data relating to navigation to network accesses would have been processed for "institutional functions" by the Director of the Territorial Management Office, by the network administrator and by the Director of the Personnel Office and would not have been "disseminated or communicated to unauthorized third parties "(see p. 3 cit. note);

- the complainant's personal data, processed in this context, are "day, time, username, PC used and site consulted"; "The request for control was made by the competent manager" and "the data was extracted by a person appointed as system administrator";

- "the data have been processed by the office and body competent in disciplinary proceedings (chapter II of the inter-departmental contract; art. 21 D.p.Reg. 01.02.2005 n. 2 / L and subsequent amendments today art. 107 of" code of local authorities "pursuant to L. R. 03.05.2018, n. 2; Title IV of Legislative Decree 30.03.2001, n. 165 and subsequent amendments; art. 42-bis of the organic regulation and organization of the Municipality of Bolzano) ";

- "the information relating to the initiation of disciplinary proceedings and their outcome against the [complainant] was provided to the lawyer of the Director of the territorial management office with a note of the XX", in response to a request for access to the documents pursuant to art. 22 and ss. of the l. 241/1990. In any case, "a copy of the documents relating to the aforementioned disciplinary proceedings was never given but only the information resulting from the note of the XX";

- "the examination by the Division Director of the request for an extraordinary visit to the competent doctor took place by law for the purposes of health surveillance requirements as in the Municipality of Bolzano, the employer is the Division Director - just resolutions of the Municipal Council n. 85/12 and n. 532/13 ";

- “the form for the request for an extraordinary medical examination is also freely filled in by the applicant and does not require an indication of the pathology suffered”; [...] "is sent directly by the person making the request to the secretariat of the competent doctor" and "at the outcome of the visit, the competent doctor transmits the certificate of suitability for the specific job [...] to the personnel office of the municipality which volta sends it by e-mail to the employer / Division Manager, so that any requirements may be fulfilled "; "A copy of the aforementioned certificate is filed in the employee's independent personal file, as required by the organizational measures adopted, to guarantee protection and particular data" (see p. 4 cit. Note); for the future, the Municipality intends to revise the form through "further minimization of data pursuant to art. 5 of the GDPR "(see p. 11, cit. Note).

With a note of the XX (prot. No. XX), the Office, on the basis of the elements acquired, notified the Municipality, 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 Regulations, inviting the aforementioned owner 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 Law no. . 689 of 11/24/1981).

With the aforementioned note, the Office found that the Municipality has put in place the processing of personal data of employees relating to internet browsing, even unrelated to the work of the interested parties, in the absence of a suitable prerequisite of lawfulness of the processing, appropriate information and an impact assessment on data protection, in a way that does not comply with the principles of lawfulness, correctness and transparency and minimization, in violation of Articles 5, par. 1, lett. a) and c), as well as in violation of articles 6, 9,13, 88 and 35 of the Regulation and of the articles 113 and 114 of the Code, also with reference to the requirements set out in Annex 1 of Provision no. 146 of 5 June 2019, doc. web n. 9124510. In addition, with regard to the processing of personal data of employees on the occasion of the request for an extraordinary medical examination, the Office found the violation of art. 5, par. 1, lett. a) as well as in violation of art. 9, paragraph 2, lett. b) of the Regulations.

With a note of the twentieth century, the Municipality sent its defense briefs, "manifesting [...] the will to cooperate with this Authority in order to remove the alleged defects", attaching the necessary documentation to prove the measures adopted for this purpose with regard to treatments in progress against the generality of employees, and specifying, among other things, that:

- "since the 20th century, orders have been given to suspend the processing of the navigation logs pursuant to the trade union agreement d.d. 25.10.2000 and subsequent amendments, by managers "(see annex no. 1);
- "the impact assessment on the protection of personal data was drawn up in relation to the processing of" browsing logs ", identifying, with respect to the current situation, a series of technical and organizational improvement measures";
- "within the navigation log files, the userid, which reported the initial of the name and first characters of the surname of the users, has been replaced by XX by a number. This measure takes the form of pseudonymisation aimed at minimizing the data processed "(see attachment no. 2);
- "A new decentralized agreement was entered into with the trade unions, in relation to the possibility of using the navigation

logs for the purposes of the so-called" unintentional checks "in compliance with the guidelines referred to in resolution 13 d.d. 01.03.2007 of this Authority and the prescriptions that emerged from the subsequent Provisions, including n. 303 d.d. 13.07.2016, as well as the safeguards referred to in Recommendation CM / Rec (2015) 5 of the Committee of Ministers of the Member States on the processing of personal data in the employment context, and the concepts that emerged during the hearing of President Antonello Soro on the of legislative decrees implementing the Jobs Act d.d. 9 and 14 July 2015 ";

- this agreement, "by limiting the hypotheses of activation of the control procedure to anomalies in relation to IT incidents and by graduating monitoring, considerably improves the protection of workers' rights and freedoms" (see Annex 3);

- "the information for internet users has been drawn up and published on the municipal intranet site, subject to prior notice to the individual user" (see Annex 4 and 5) and the information provided pursuant to art. 13 of the Regulations "for the employee and municipal collaborator" (see annex no. 44);

- "[...] the request form [for an extraordinary visit] was immediately replaced, with the elimination of the" employer "manager's visa (see annex no. 6);

- with regard to the specific processing of the complainant's data, “the episodes referred to in the complaint in reference to the navigation logs concerned the control of the navigation logs of an employee for a period of days. 30, in the presence of gradual checks through the work tools not fully compliant with the prescriptions of this Authority. In fact, the Municipality has put in place measures to prevent controls (differentiated internet access, filters and blacklists, and 2 circulars addressed to all staff, respectively d.d. 15/03/2017 and 12/05/2017 - annexes 7, 8, 9 -), which were already taking shape gradually; the control only in the final phase, at the time of the request by the manager to acquire the internet browsing reports [of the interested party], did not satisfy the graduality ";

- "the information on the processing was contained in various documents, partly available on the municipal intranet, partly contained in the general information for personnel, available not on the municipal website, but posted since 2004 in each office, in compliance with circular d.d. 12.08.2004 "(see annex nos. 10, 11, 12, 13, 14 in the documents);

- "there was an agreement stipulated pursuant to art. 4 of Law 05.20.1970, n. 300 and subsequent amendments, with the trade unions on 25.10.2000, supplemented by subsequent agreement d.d. 25.03.2010 [… which provided for] a summary balance between the growing need to use the internet, and the disadvantages that could ensue [… even if] subsequently they were not perfectly aligned with the resolution of the Guarantor no. 13 d.d. 01.03.2007 "Guidelines for e-mail and internet", and

subsequent measures "(see attachment no. 10);

- "the purpose of the processing of the navigation logs at the time of the disputed facts, pursuant to art. 22 of Legislative Decree. 30.06.2003, n. 196 was identified in the technical measures to be used to safeguard the data processed, respectively by art. 14bis and 71 of the CAD "Digital Administration Code", approved by Legislative Decree 07.03.2005, n. 82 and subsequent amendments, and the Directive of the President of the Council of Ministers 01.08.2015 "Minimum ICT security measures for public administrations"; "The further purpose of the control treatment of the worker by the manager was based on articles 54 and 55 sexies, paragraph 3 and of the Legislative Decree. 30.03.2001, n. 165 and subsequent amendments ";

- "from the entry into force of the GDPR 2016/679 to 03.02.2020, the legal basis of the" non-intentional "control treatment was established, pursuant to art. 9, paragraph 2, letter b), of the GDPR, from the decentralized agreement with the most representative trade union organizations within the Municipality of Bolzano d.d. 25.10.2000, as supplemented by the subsequent d.d. 25.03.2010 "(see annex nos. 10 and 15);

- "the Code of Conduct of the Municipality of Bolzano, approved with a resolution of the City Council 608 d.d. 30.10.2015, which in art. 10 deals with IT security, is recalled as a fundamental tool for the prevention of corruption by point 8.3 of the three-year plan for the prevention of corruption and for transparency 2020-2022 approved with the resolution of the City Council 27.12.2019, n. 827 "(cf. all. Nos. 16,17, 18);

- "From 2010 to today, 15 control requests have been processed, [...] which involved 27 users of municipal IT tools, one of which resulted in the imposition of a disciplinary sanction, and one in the initiation of a proceeding disciplinary, however filed "(relating to the complainant);

- "from the XX, unchanged the rest, the legal basis of the" unintentional "control treatment is constituted, pursuant to art. 9, paragraph 2, letter b), of the GDPR, by the new decentralized agreement d.d. 04.02.2020, stipulated following discussions with the trade unions ";

- "the episode referred to in the complaint led to the acknowledgment of the request to be subjected [or] to an extraordinary medical examination formulated by the employee by his manager," employer "on the basis of the municipal safety organization chart on the work [...] The specific request procedure was also designed in relation to the preventive health surveillance functions assigned to the manager [... to] identify, as a precautionary measure and in consultation with the employees, where requested by the interested parties, a better or different working method compatible with the inconvenience pending any

prescriptions from the competent doctor ";

- "the employer must in any case be made aware of a medical examination, even if on the employee's initiative, by virtue of public accounting rules, where, in the settlement of the fees to the competent doctor , must verify the correctness and adequacy of the amounts invoiced to the Municipality "; "From 2014 to date the requests submitted by municipal employees have been n. 19 "(see annex no. 20).

The hearing requested by the Municipality was also held on the 20th, pursuant to art. 166, paragraph 6, of the Code, on the occasion of which, in confirming what has already been declared in the defense briefs, it was represented, among other things, that:

- "the Municipality has for a long time paid attention to compliance with the legislation on the protection of personal data [...], adopting specific organizational and procedural measures, also to ensure the protection of the interested parties, always operating in full transparency towards the latter ";

- "at the time when the facts subject of the complaint occurred, the Municipality found itself facing various regulatory changes in various areas [...] at the same time as problems in the management staff" as well as "difficulties in interpreting the regulatory framework in force on the subject of protection some data";

- "now the Municipality has reached a better level of compliance with the legislation on the protection of personal data, also with regard to compliance with the principles of data protection by design and by default and the execution of impact analyzes of the treatment"

- "if there has been a violation, it must still be considered slight. The Municipality had in fact reached a trade union agreement pursuant to art. 4 of the Workers' Statute, which expressly provided for the prohibition for workers to use IT tools for personal purposes. This also in consideration of the public nature of the employer. [...] If personal use was precluded, there was, therefore, no problem of personal data protection upstream, since the presence of data unrelated to the work activity was not foreseen. Furthermore, in terms of the number of logs and the number of workers involved, the violation, if any, is minor even in quantitative terms ";

- "the logs did not lead to the application of disciplinary sanctions, as they were not reliable, also reporting a series of sites (eg connected to banners) that had not necessarily been visited by the worker, without the possibility of distinguishing between the site actually visited and those with indirect / involuntary navigation. For the same reason, even the browsing time on these

sites was not reliable information for disciplinary purposes ";

- “the Municipality has provided further information and instructions to workers on how to use the IT tools, improving overall the level of compliance with current legislation with regard to the collection of navigation log files. In particular, the logs, which previously reported the "user id" explicitly, now no longer report this information but only a "machine id", which allows to trace the user's identity only with subsequent processing, by carrying out the combination between the "machine id" and the worker to whom this machine is assigned. In this way, the personal data collected was pseudonymised. Moreover, the logs are kept for only 30 days and are processed, matching them to the user's identity, only if there are anomalies such as to suspect a threat to IT security (for example, excessive traffic above the norm, which can cause think of an attack on the machine; a repetitive access to a single site, which can lead to believe that the machine is operating independently of the user's will). It is therefore the office responsible for IT security that detects anomalies and requests further information. […]. In any case, the logs are useless for the purpose of unintentional control, because they consider navigation times as a whole and do not distinguish between intentional and involuntary navigation. Furthermore, it is pointed out that all the preparatory activities to prevent employees from visiting unsafe sites had already been implemented ";

- as regards the profile of the complaint relating to the request for a medical examination for psychological support "[...] it was essential that employees inform their managers of any situations of personal distress in relation to health or safety, also to prevent any accidents and / o illnesses pending the execution of the medical examination, modifying the assignment of the tasks and activities assigned to the employee who makes the request for the visit or the methods of performance of the working activity. The request for a visit, however, does not enter into the merits of the specific alleged pathology, because it is not motivated by the worker, as there is therefore no processing of personal data relating to health. In any case, the Municipality has now provided in the new forms that the manager no longer has to be informed of the request for an extraordinary visit ”;

- "as regards the contestation of the failure to carry out the impact assessment of the processing, it is believed that it was not mandatory, given that there are at least two of the criteria indicated by the European Data Protection Committee to identify the cases in which it it is mandatory. Furthermore, when the Guarantor indicated in the 2018 provision the cases in which the assessment is mandatory, it, by recalling the criteria referred to in points 3.7 and 8 of the Guidelines of the Committee, implicitly excluded from the obligation the cases of treatment related to the use of work tools. The evaluation cannot, therefore,

be considered mandatory in relation to processing related to the use of tools necessary for work performance. It is noted, however, that the provision of the Guarantor is difficult to interpret and that its practical application is problematic in the various contexts, having, moreover, been issued after the facts which are the subject of the complaint ".

3. Outcome of the preliminary investigation.

The personal data protection discipline allows the employer to process personal data, also relating to particular categories of data (see Article 9, paragraph 1, of the Regulation), of workers in compliance with the general principles of processing (Article 5 of the Regulation) and if the processing is necessary to fulfill specific obligations or tasks provided for by national or Union legislation, in particular for the purpose of managing the employment relationship (Article 6, paragraph 1, letter c), 9, para. 2, lett. b), and 4, and 88 of the Regulation) or "for the performance of a task of public interest or connected to the exercise of public authority vested in the data controller" (Article 6, paragraph 1, lett . c) and e), of the Regulation and 2-ter of the Code).

The employer must also comply with national regulations, which "include appropriate and specific measures to safeguard human dignity, legitimate interests and fundamental rights of the data subjects, in particular as regards [... the use of] monitoring systems in the workplace "(articles 6, par. 2, and 88, par. 2, of the Regulations). On this point, the Code, confirming the system prior to the changes made by Legislative Decree 10 August 2018, n. 101, expressly refers to the national provisions of the sector that protect the dignity of people in the workplace, with particular reference to possible controls by the employer (articles 113 "Data collection and relevance" and 114 "Guarantees regarding remote control "). In particular, art. 114 of the Code provides that "Without prejudice to the provisions of Article 4 of Law May 20, 1970, n. 300 ", similarly to art. 113 which refers to art. 8 of the l. May 20, 1970, n. 300, and art. 10 of Legislative Decree 10 September 2003, n. 276.

These rules constitute in the internal system those more specific and greater guarantee provisions referred to in art. 88 of the Regulation - for this purpose the subject of a specific notification by the Guarantor to the Commission, pursuant to art. 88, par. 3, of the Regulation -, the observance of which constitutes a condition of lawfulness of the processing and the violation of which - similarly to the specific processing situations of Chapter IX of the Regulation - also determines the application of administrative pecuniary sanctions pursuant to art. 83, par. 5, lett. d), of the Regulation (cf., with regard to the public sector of work, provision no. 90 of 11 March 2021, currently being published; provision no. 53 of March 5, 2020, web doc. no. 9433080; but see also provision no. 167 of 19 September 2019; see also the jurisprudence of the European Court of Human Rights, in the case of Antovic and Mirković v. Montenegro (Application no. 70838/13 of 28.11.2017), which established that respect for

"private life" must also be extended to public workplaces, highlighting that workplace checks can only be carried out in compliance with the guarantees provided for by the applicable national law).

The data controller is, however, required to comply with the principles of data protection (Article 5 of the Regulation) and is responsible for the implementation of the technical and organizational measures appropriate to guarantee and be able to demonstrate that the processing is carried out in compliance with the Regulations (articles 5, par. 2, and 24 of the Regulations).

3.1. The principle of lawfulness, correctness and transparency of the processing of data relating to employee Internet browsing: information to interested parties.

In compliance with the principle of "lawfulness, correctness and transparency", the data controller must take appropriate measures to provide the data subject with all the information referred to in Articles. 13 and 14 of the Regulations in a concise, transparent, intelligible and easily accessible form, with simple and clear language (Article 12 of the Regulations).

In light of the evidence, the Municipality has adopted, since 2000 (see trade union agreement of 20.10.2000 for the use of network services, integrated on 25.3.2010, limited to some aspects), a system that allows the generalized (and ex ante) tracking of Internet access by employees and the storage, for thirty days, of information of a personal nature ("day, time, user name, PC used and site consulted").

Originally, in the navigation log files "the userid [...] reported the initial of the name and first characters of the surname of the users" then replaced ("from XX") "with a number corresponding to the machine id" (cf. . note XX and minutes of hearing XX, cit.). The system therefore made it possible, through the possibility of tracing navigation to a specific user name ("user id"), to carry out an individualized control of the Internet browsing of individual employees, by extracting data by the network administrator , at the request of the competent managers. So much so, in order to "generate evidence for the IT security of the Municipality network", the integrity of which should be ensured to allow the execution of the public interest tasks of the Authority (art. 6, par. 1, lett.), of the Regulation).

During the investigation, the Municipality declared that it had provided employees with general information on the processing of personal data prior to the entry into force of the Regulation and that it had prepared another, updated to the new regulatory framework, "published in the institutional site ". However, during the checks it emerged that, on the website of the Entity, there was no specific information relating to the processing of personal data of employees nor, in those made available, was there

any reference to the processing of personal data relating to navigation. on the Internet by them.

A reference to the tracing operations of Internet connections was instead present in other documents made available to employees, some of which published on the intranet, such as the trade union agreement, the code of conduct, some internal circulars of the Personnel Office, as well as the form that each employee had to sign when applying for access to the Internet and other network services. These documents, which did not however contain all the essential information required by art. 13 of the Regulation, having been drawn up to fulfill obligations other than those deriving from the data protection regulations, cannot therefore replace the information that the owner must make, before starting the treatment, to the interested parties regarding the characteristics essential of the same; this in order to allow the interested party to be fully aware of the type of processing operations that may be carried out also by drawing, within a framework of lawfulness, on the data collected during the work activity (see, Judgments of the European Court of Rights of the Man of September 5, 2017 - Appeal n. Ribalda and others see Spain, spec. Par. No. 115). On this point, it should also be noted that the fulfillment of the information obligations towards the employee (consisting of "adequate information on how to use the tools and perform controls") constitutes a specific condition for the lawful use of all data collected during the employment relationship, through technological tools and / or work tools, for all the purposes connected to the related relationship, including disciplinary findings, together with compliance with the regulations on the protection of personal data (see art. 4, paragraph 3, law no. 300 of May 20, 1970).

However, it is acknowledged that, after the initiation of the procedure, the Municipality has drawn up a specific information dedicated to the treatments which, for organizational and IT security needs, entail the tracking of employee activities as documented in the defense briefs (see annex no. 12 to the note of the XX).

Therefore, until the adoption of the new information document for employees (dated XX), the processing appears to have been carried out in violation of the obligation set out in art. 13 of the Regulation, as well as - given the fragmentation of the information contained in multiple acts, different in nature and function, stratified over time by the administration - not in accordance with the principle of correctness and transparency and therefore in violation of Articles 5, par. 1, lett. a), and 13 of the Regulations.

3.2. The principle of data minimization and the collection of non-work related data.

According to the Regulation, the processing must be "necessary" with respect to the lawful purpose pursued (Article 6, par. 1 of the Regulation) and have as its object only the data "adequate, relevant and limited to what is necessary with respect to the

purposes for which are processed "(art. 5, par. 1, letter c), of the Regulation).

As emerges from the documents, the system adopted by the Municipality for network security purposes, in the original configuration, allowed filtering and tracing of connections and links to external Internet sites, the storage of such data and their conservation, for thirty days. , as well as the extraction of reports, even on an individual basis. Based on an overall assessment of the elements that emerged during the investigation, it appears that the processing of personal data collected and processed by the Municipality through authorized personnel and system administrators ("day, time, site consulted"), in the presence of a direct and univocal connection with the employee and with his specific workstation (as the data collected also included "user name and PC used"), gave rise to a systematic collection of data relating to the activity and use of network services by directly identifiable employees.

In this context, the administration entered into an agreement with the trade unions - first in 2000, then updated in 2010 and, most recently, on XX 2020 (see attachment no.11, note of XX, in documents) - as prescribed by the regulations on the use of technological systems in the workplace (article 4 of law no. 300 of 1970) which, also following the amendments established by legislative decree no. 151, allows the use of "audiovisual systems and [of] other tools from which also derives the possibility of remote control of the activity of workers [...] exclusively for organizational and production needs, for work safety and for the protection of of company assets ", in compliance with specific conditions, such as prior agreement with the unitary union representation or company union representatives, or, alternatively, with prior authorization from the local offices of the National Labor Inspectorate (paragraph 1). Moreover, the Guarantor, after the changes made in 2015 to this sector framework, also expressed its opinion, precisely with regard to the use of systems that involve tracing access to the Internet (see provision of 13 July 2016, no. 303 web doc. 4, paragraph 1 of the l. 300 of 1970, not being able to be included in the category of "work tools", pursuant to art. 4, paragraph 2, unlike the systems of automatic inhibition of the consultation of contents on the net

In any case, the data controller must always respect the principles of data protection (Article 5 of the Regulation). This implies that the scope of the controls (indirect or unintentional), within the limits established by the sector regulations, and the processing of personal data that can be lawfully carried out by the employer, must in any case be non-massive, gradual and admissible only after an experiment. of less restrictive measures of workers' rights (see Hearing of the Guarantor on the Jobs Act at the Labor Commission Chamber of Deputies 9 July 2015, web doc. Strasbourg "- ECHR, judgment 17 October 2019, López Ribalda and others v. Spain-, web doc. 9164334," the essential requirement for workplace controls, including defensive

ones, to be legitimate therefore remains, for the Court, the their strict proportionality and not excess: cornerstones of the data protection regulations whose "social function" is confirmed, also from this point of view, more and more central because ce to combine dignity and economic initiative, freedom and technique, guarantees and duties ").

Considering that the borderline between the working and professional sphere and the strictly private one cannot always be clearly drawn, the cancellation of any expectation of confidentiality of the interested party in the workplace cannot be prefigured, even in cases where which the employee is connected to the network services made available to the employer or uses a company resource also through personal devices, which is why the European Court of Human Rights has confirmed over time that the protection of private life (art. 8 European Convention on Human Rights) also extends to the workplace, where the personality and relationships of the person who works are expressed (see Judgments of the European Court of Human Rights Niemietz v. Allemagne, 16.12. 1992 (ref. No. 13710/88), spec. Para. 29; Copland v. UK, 03.04.2007 (ref. No. 62617/00), spec. Para. 41; Bărbulescu v. Romania [GC], 5.9 .2017 (ref. No. 61496/08), spec. Paragraphs 70-73 and 8 0; Antović and Mirković v. Montenegro, 28.11. 2017 (ref. No. 70838/13), spec. par. 41-42). Therefore, the processing of data carried out using information technology, in the context of the employment relationship, must comply with respect for fundamental rights and freedoms as well as the dignity of the interested party, for the protection of workers and third parties (see Recommendation CM / Rec (2015) 5 of the Committee of Ministers to the Member States on the processing of personal data in the employment context, spec. Point 3).

With regard to the present case, according to what emerges from the documents and confirmed by the data controller, it appears instead that the original characteristics of the system and the consequent processing operations (preventive and generalized collection of data relating to connections to the websites of individual employees, storage for thirty days and the possibility of extracting reports relating to the navigation of individual employees) were not necessary and proportionate with respect to the purpose of protection and security of the internal network invoked by the Entity (see recital 49 and art. 6, paragraph 1, letter e) of the Regulation), having also concerned data that were not "adequate, relevant and limited" to what is necessary to guarantee network security, in violation of the principles of lawfulness and minimization pursuant to art. 5, par. 1, lett. a) and c), and of art. 6 of the Regulation (see provision no. 303 of 13 July 2016, web doc. 5408460, par. 5, cit .; on this point, see also Council of Europe, Recommendation of 1 April 2015, CM / Rec (2015) 5, princ. Spec. 15; Article 29 Working Party, Opinion No. 2/2017 on data processing in the workplace, WP 249, para. 5).

From this point of view, however, the system used by the Entity made it possible to record detailed data regarding the internet resource visited (URL), which, precisely because of the unique connection with the employee's name, gave rise to the systematic collection of numerous personal data, also not relating to the performance of work, and information relating to the private life of the interested party.

The system used by the Municipality by carrying out a systematic collection of employee navigation data inevitably involved the processing of information also unrelated to professional activity, inferable from the URLs visited, and was therefore in contrast with the prohibition for the employer to process data "not related to the evaluation of the professional aptitude of the worker" and therefore with art. 113 of the Code, with reference to art. 8 of the l. May 20, 1970, n. 300 and art. 10 of Legislative Decree 10 September 2003, n. 276 (see, on the point Provision of the Guarantor no. 308 of 21 July 2011, web doc. No. 1829641, confirmed by the Court of Cassation, sentence no. 18302 of 19 September 2016, where it is read that "the acquisition and retention of data relating to the Internet browsing of employees by [...] recording the log files also implies the violation of the provisions of law no. 300 of 1970, art. 8 "and that" acquire and store data that contain (or may contain) such information already involves the integration of the prohibited conduct [...] even if the data are not subsequently used. It is not necessary to subject the collected data to any particular treatment to incur the offense, since the mere acquisition and conservation of the availability of they involve the violation of the legislative prescription ").

The need to reduce the risk of improper use of Internet browsing by employees, consisting of activities not related to work performance (for example, viewing irrelevant websites, uploading or downloading files, 'use of network services for recreational purposes or unrelated to work) cannot, in fact, justify any form of interference in private life, but can be satisfied through the provision of technical and organizational measures suitable for preventing any information relating to non-working sphere are collected, giving rise to the processing of personal information, "irrelevant" that fall within the scope of application of art. 113 of the Code (with regard to the risks for the interested parties and the responsibilities for the owner in relation to the acquisition of information relating to the private sphere of employees, see lastly, provision of 15 April 2021 no. 137 being published; but see also, provision of 26 March 2020, n.64 - "Distance learning: first indications" -, web doc. n. 9300784, par. 13 of 1 March 2007, web doc. 1387522 in particular, point 5.2., Letter a), the principles of which can still be considered valid).

From another point of view, however, it is not specifically proven by the documents that, in this case, data relating to particular categories have actually been processed in violation of the provisions of the Provision of the Guarantor no. 146 of 5 June 2019

(containing the provisions relating to the processing of particular categories of data, pursuant to Article 21, paragraph 1, of Legislative Decree 10 August 2018, no. 101, web doc. 9124510 and in G. U., 29.7.2019, n.176), therefore the survey on this point having to be filed with regard to this specific profile.

3.3. The principle of purpose limitation and failure to comply with the conditions laid down by the sector regulations with regard to the use of the data collected for other purposes related to the management of the employment relationship.

Given the principle according to which the data must be "collected for specific, explicit legitimate purposes, and subsequently processed in a way that is not incompatible with these purposes" (Article 5, paragraph 1, letter b), of the Regulation) it should be noted that the Municipality has reserved, since 2000, the possibility of consulting the data relating to the web browsing of its employees, at the request of the competent manager and through the system administrator, for any needs related to disciplinary proceedings. This has actually happened against certain employees (indicated by the Municipality in the number of 27 workers), including the complainant, with consequent use of the data collected by the system as part of the disciplinary procedure against the same.

In the premise that, only since 2015, the current regulatory framework allows the data collected pursuant to art. 4, paragraphs 1 and 2 of law no. 300/1970 can be used by the employer "for all purposes related to the employment relationship" on condition that "the worker is given adequate information on how to use the tools and carry out controls and in compliance with the provisions of Legislative Decree No. 196 of 30 June 2003 "(Article 4, paragraph 3 of Law No. 300/1970), the following is noted.

The aforementioned regulatory framework therefore allows the owner (employer) to use, for further processing necessary for the management of the employment relationship, only the information collected in compliance with the conditions and limits provided for by art. 4, paragraphs 1 or 2, of the l. n. 300/70 and the data protection regulations. Such subsequent and any processing operations therefore presuppose the need to provide the interested parties with adequate information on the treatments that the employer reserves the right to carry out and the appropriate configuration of the systems so that only the necessary and collected operations are carried out. only the relevant data in relation to the main purpose for which the data are originally processed (on this point, see Provv. 24 May 2017, n. 247, web doc. n. 6495708, spec. point 5.3 and letter e) of device). In other words, the current regulatory framework allows the employer to use the personal data of workers for further purposes attributable to the management of the relationship (see the example contained in Article 88 of the Regulation) within

the limits of which the original collection was lawfully carried out, having regard to the main purpose and in compliance with the general principles of data protection.

In the present case, however, it appears that the data relating to the complainant's web browsing, originally collected and processed through the aforementioned system in a way that is not proportionate and does not comply with the regulations on the protection of personal data, in violation of art. 5, par. 1, lett. a) and c), 6 of the Regulations and art. 113 of the Code, and without adequate information pursuant to art. 13 of the Regulation, were subsequently used to contest disciplinary charges against the same, thus not respecting the conditions and conditions set out in the aforementioned sector regulations in art. 4, paragraph 3, of law no. 300 of 1970.

During the investigation, the owner stated that the analysis of the logs relating to the navigation of the interested party "did not lead to the application of disciplinary sanctions, as they were not reliable, also reporting a series of sites (eg. Linked to banners) that had not necessarily been visited by the worker, without the possibility of distinguishing between the site actually visited and those with indirect / involuntary navigation. For the same reason, even the browsing time on these sites was not reliable information for disciplinary purposes "(see, hearing report XX). Contrary to what the data controller claims, however, it is believed that the circumstance on the basis of which, given the poor quality of the data collected and their ascertained unreliability, cannot be considered relevant, in order to exclude the liability of the same, disciplinary procedure was subsequently filed, given that, in any case, the data relating to the complainant's web browsing (similar to what happened in the previous 27 cases as confirmed by the Municipality) were in any case used to initiate the aforementioned disciplinary procedure and processed in within the scope of the same, not respecting the prerequisites and conditions provided for by the aforementioned sector regulations in art. 4, paragraph 3, of law no. 300 of 1970, therefore, in violation of articles 5, par. 1, lett. a), 6 and 88 of the Regulations and in violation of art. 114 of the Code in reference to art. 4, paragraph 3, of law no. 300 of 1970.

3.4. The current processing of data relating to employee internet browsing.

In acknowledging the fact that the owner, following the dialogue with the Authority, has stipulated a new trade union agreement and modified the type of web browsing data collected, providing for new procedures for the activation of checks on employee traffic only in the presence of anomalies detectable by the network administrators (see note of the XX relative annexes as well as the minutes of the hearing of the XX), further observations are formulated below.

The methodology identified by the Entity, aimed at minimizing the data processed ("the logs, which previously reported the" user id "explicitly, now no longer report this information but only a" machine id ", which allows to go back to the 'identity of the user only with a subsequent processing, by matching the "machine id" and the worker to whom this machine is assigned. In this way, the personal data collected have been pseudonymised "- see the minutes of the hearing of the XX), it cannot yet be considered sufficient to make the overall processing proportionate and to minimize the personal data collected, being, instead, a mere pseudonymisation, as defined in art. 4, point n. 5, of the Regulation, of the personal data in question. The measures introduced by the administration still allow the administration to collect the navigation data individually and to associate these data with the data subject, albeit through indirect and, moreover, simple processing, since the workstation is assigned. almost exclusively to the employee, that the presence of any workstations shared between several people is to be considered a residual circumstance and that, even in this limited case, it is always possible to identify the user of the workstation in a given period of time. This is, moreover, confirmed by what is reported in the agreement signed on February 4, 2020, according to which "these logs, albeit pseudonymized in the user id, allow secondary control".

The measure introduced, therefore not guaranteeing adequate separation between Internet browsing data (including in particular the URL visited) and the identities of employees, cannot therefore be considered adequate to ensure compliance with the data protection regulations. , with particular regard to the principles of lawfulness, correctness and transparency, and minimization, as well as the specific provisions that prohibit the employer from acquiring, even incidentally, data relating to the employee's non-working sphere (Article 113 of the Code).

Nor can it be considered sufficient, for this purpose, for the employer to limit himself to recalling the correct use of the network tools by his employees, as reported in the trade union agreement and in the disclosure (see Annex 11 and 12 to the note of the XX), relying exclusively on the responsibility of employees and on the prohibition of the use of information tools for personal purposes ("it is of fundamental importance that the worker strictly adheres to the instructions for the use of IT tools and the Code of behavior approved with the resolution of the Council d.d. 30.10.2015, n.608, so that the logs being processed do not reveal information that pertains to your extra-professional private sphere, and / or to the categories of data referred to in articles 9 and 10 of the GDPR 2016/679 ").

For these reasons, it is believed that the proposed adjustments do not allow to completely overcome, at present, the criticalities highlighted and that, therefore, the treatment in progress must still be considered not fully compliant with the

regulations on the protection of data.

3.5. Failure to perform a data protection impact assessment.

In implementation of the principle of accountability (which requires the adoption of adequate technical and organizational measures to ensure that the processing takes place in compliance with current legislation; see articles 24 and 25 of the Regulation), it is up to the owner to assess whether the treatments that are intended to present a high risk for the rights and freedoms of individuals - due to the technologies used and considering the nature, object, context and purposes pursued - which requires a prior impact assessment on the protection of personal data.

The processing of the personal data of the data subjects was carried out in the absence of a preliminary impact assessment on data protection on the assumption that the processing did not present specific risks for them.

Taking into account the information provided also at European level on this point, it is noted, however, that the processing made possible by the system described, as configured, consists of the preventive and generalized collection of data relating to connections to the websites of individual employees (originally associated directly to the name, to date, through the machine ID), in the storage for thirty days and in the possibility of extracting a report relating to the navigation of individual employees, involves specific risks for the rights and freedoms of the data subjects in the working context (art.35 of the Regulation).

So in consideration of the particular "vulnerability" of the data subjects in the workplace (see recital 75 and art. 88 of the Regulation and the "Guidelines concerning the impact assessment on data protection as well as the criteria for establishing whether a treatment" may present a high risk "pursuant to Regulation 2016/679", WP 248 of 4 April 2017, which, among the categories of vulnerable data subjects, expressly mentions "employees") and of the fact that in this context the use of systems involving "Systematic monitoring", understood as "processing used to observe, monitor or control data subjects, including data collected via networks" (see criterion no. 3 indicated in the Guidelines, cit., But also see criteria 4 and 7) , may present risks, as emerged in the present case, in terms of possible monitoring of employee activity (see articles 35 and 88, paragraph 2, of the Regulation, see also Provision of the Guarantor of 11 October 2018, n. 467, doc. web n. 9058979, annex n. 1, which expressly mentions the "processing carried out in the context of the employment relationship using technological systems [...] from which it derives the possibility of carrying out a remote control of the activity of employees").

For these reasons, in acknowledging that, albeit belatedly and during the investigation, the owner has carried out the impact assessment on the protection of personal data in relation to the processing of "navigation logs", identifying a series of

measures technical and organizational with the intent to mitigate the risks for the data subjects deriving from the treatment (see annex bearing the date XX, in note XX), it is believed that, at least with regard to treatments prior to the month of XX, the treatment has been carried out in the absence of an impact assessment and therefore in violation of art. 35 of the Regulation.

3.6. The processing of personal data related to the request for an extraordinary medical assessment under the so-called "Health surveillance" (legislative decree 9 April 2008, no. 81).

With regard to the processing of the complainant's data carried out through the request form for an extraordinary medical examination, the following is noted.

The purpose of safety and health in the workplace typically relates to the fulfillment of obligations regarding "labor law", which legitimize the processing of personal data of employees by the employer (articles 5, 6, par. 1, lett. c), 9, par. 2, lett. b), and 88 of the Regulations) and of the competent doctor (Article 9, paragraph 2, letter h), and 3, of the Regulations; cf. also art. 2-sexies, paragraph 2, lett. u), of the Code), each within the scope of the different tasks and within the precise limits set by law. This also within the framework of the more specific national provisions of greater protection which guarantee the dignity and freedom of the employee in the working context (articles 88 of the Regulation and 113 of the Code).

Therefore, while the employer "ensures that the workers [...] are not assigned to specific work duties without the required suitability judgment" (eg Article 18 of Legislative Decree no. 81/2008), the competent doctor , as part of its health surveillance activities ("health surveillance is carried out by the competent doctor"), is the only person entitled to process data relating to the health of workers and to verify suitability for the "specific task" (Articles . 25, 39, paragraph 5, and 41, paragraph 4, of Legislative Decree no. 81/2008), being able, "according to the risk assessment" and the "health conditions" of the workers, to establish the need for subject workers to further diagnostic investigations; it is also envisaged that the worker can contact the competent doctor directly to obtain an extraordinary visit related to his specific or supervening health conditions (Article 41, paragraphs 2 and 4, of Legislative Decree 81/2008).

On the basis of the aforementioned regulatory framework, the employer can know the mere judgment of suitability for the specific job accompanied by any requirements that the professional establishes as working conditions (see Article 41, paragraph 6-bis, of Legislative Decree no. 81/2008). Therefore, only once the visit has been carried out, the employer must, on the basis of the regulatory framework outlined above, implement any measures indicated by the competent doctor and assign the worker to the corresponding duties (Article 42 of Legislative Decree No. 81 / 2008).

On the other hand, it is not envisaged that, as proposed by the Municipality, "pending the completion of the medical examination" the employee informs his / her manager of "any situations of personal distress" in order to obtain the "modification [... of] the assignment of tasks and activities assigned to the employee making the request for a visit or the methods of performance of the working activity "(see minutes of hearing in documents).

Nor can this treatment be justified by the need to "verify the correctness and congruity of the amounts invoiced to the Municipality" (see minutes of the hearing in documents), it being envisaged that the doctor "communicates [who] to the employer [...] the collective anonymous results of health surveillance "(see art. 25, paragraph 1, letter i), of Legislative Decree no. 81/2008), which may possibly be used, in the absence of other elements, when accounting for the activity carried out and the payment of the fees to the competent doctor.

Having said this, it is believed that the form originally used by the administration, which the employee had to fill in to request the competent doctor for an extraordinary assessment of their health conditions, in the part in which it required the necessary acknowledgment of the Department Manager, not complies with the aforementioned sectoral regulatory framework resulting - regardless of the express indication of the pathology by the worker - that subjects delegated to carry out employer functions within the administration, become aware of personal data relating to the state of health, different and further than those permitted by law, being, therefore, the processing of personal data of workers who have filled out this form occurred in violation of Articles 5, 9, par. 2, lett. b), and 88 of the Regulation.

4. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the data controller in the defense writings whose truthfulness may be called upon to answer pursuant to art. 168 of the Code. the act of initiation of the proceeding and are therefore insufficient to allow the filing of this proceeding, since none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

From the checks carried out on the basis of the elements acquired, also through the documentation sent by the data controller, as well as from the subsequent evaluations, the non-conformity of certain treatments concerning the personal data of employees was ascertained. Both with regard to both the previous regulations (ie the Code, in the text preceding the changes made by Legislative Decree 10 August 2018, n. 101), and the current regulations on data protection.

In order to determine the applicable law, in terms of time, the principle of legality referred to in art. 1, paragraph 2, of the l. n.

689/1981, according to which the laws that provide for administrative sanctions are applied only in the cases and times considered in them. This determines the obligation to take into account the provisions in force at the time of the committed violation, which in the case in question - given the permanent nature of the alleged offenses - must be identified in the act of cessation of the unlawful conduct. In acknowledging that, limited to some behaviors, the cessation of unlawful processing took place after the date on which the Regulation became applicable (see note of the XX, in which account is taken of the various initiatives taken by the owner to remedy the violation disputed), while, with regard to the collection of Internet browsing data, the unlawful processing is still ongoing, it is believed that the Regulation and the Code constitute the legislation in the light of which to evaluate the conduct complained of in the complaint.

The preliminary assessments of the Office are therefore confirmed and the unlawfulness of the processing of personal data carried out by the Municipality of Bolzano is noted, as it occurred in a manner that did not comply with the general principles of processing, as well as in violation of Articles 5, par. 1, lett. a) and c), 6, 9, 13, 35, 88 of the Regulation, as well as art. 113 and 114 of the Code.

The violation of the aforementioned provisions entails, pursuant to art. 2-decies of the Code and "except as provided for in Article 160-bis", the unusability of the personal data processed.

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

5. Corrective measures (art. 58, par. 2, letter d), of the Regulation).

Taking into account what is represented in relation to the collection of data relating to web browsing associated with employees, albeit indirectly identifiable, also following the measures introduced starting from 17 January 2020, due to the unlawfulness of the processing in progress, it is considered necessary for pursuant to art. 58, par. 2, lett. d), of the Regulations, to order the Municipality of Bolzano, within sixty days of notification of this provision, to adopt suitable technical and organizational measures to anonymize the data relating to the employees' workstations detected in the web browsing logs as well as to delete the personal data present in the web browsing logs already recorded.

Without prejudice to the possibility of carrying out surveys of precise internet browsing data, only in the event of web traffic anomalies whose extent is such as to compromise the security and integrity of the information systems, according to what is partly provided for by the procedures last identified and included in the trade union agreement of 4 February 2020 (points 2-6),

which must be appropriately updated for this purpose.

Pursuant to art. 157 of the Code, the Municipality must also communicate to this Authority the initiatives it intends to undertake to ensure that the treatments comply with the data protection regulations, within thirty days of notification of this provision.

6. Adoption of the injunction order for the application of the pecuniary administrative sanction and ancillary sanctions (Articles 58, paragraph 2, letter i), and 83 of the Regulations; 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 Regulation, in the present case - also considering the reference contained in art. 166, paragraph 2, of the Code - the violation of the aforementioned provisions is subject to the application of the same administrative fine provided for by art. 83, par. 5, of the Regulation.

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.

For the purposes of applying the sanction, it was considered that the treatment consisting of the systematic and preventive collection of personal data relating to internet browsing involved all employees of the Municipality (about a thousand) and that, in some cases (No. 27 and between these the complainant), the data have been used for specific consultations by extracting detailed reports of the employees' web browsing, in violation of the general principles of treatment and of the national provisions of the sector that specifically protect the dignity of the data subjects in the workplace (88 of the Regulations, as well as Articles 113 and 114 of the Code). The long time span of the treatment, undertaken since 2000, was also considered.

On the other hand, it was considered that the Municipality showed a particular collaboration during the preliminary investigation by making, already following the first request for elements of the Office, some first corrections to the treatments object of the complaint and to initiate, at the same time, the necessary investigations functional to the progressive adoption also of the technical and organizational measures which, although not sufficient to ensure full compliance of the treatments with the

provisions on data protection, nevertheless denote a particular commitment to mitigate the negative effects of the treatment towards of employees. For the purposes of measuring the overall sanction, it was also considered that the data controller had trusted in the lawfulness of the treatments put in place having fulfilled the obligations established by the sector regulations, stipulating, since 2000, an agreement with the trade unions, the content of which however, it concerned processing which, during the investigation, did not comply with the principles of data protection.

Furthermore, there are no previous violations committed by the data controller or previous measures 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 € 84,000 (eighty-four thousand) for the violation of Articles 5, par. 1, letters a) and c), 6, 9, 13, 35, 88 of the Regulation, as well as art. 113 and 114 of the Code.

Taking into account the particular delicacy of the illegally processed data, 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 by 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

detects the unlawfulness of the processing carried out by the Municipality of Bolzano for violation of Articles 5, 6, 9, 88 and 35 of the Regulation, as well as 113 and 114 of the Code in the terms set out in the motivation and declares pursuant to art. 2-decies of the Code, the unusability of data processed in violation of the relevant regulations on the processing of personal data, except as provided for by art. 160-bis of the Code;

ORDER

to the Municipality of Bolzano, in the person of the pro-tempore legal representative, with registered office in Bolzano, Piazza Municipio, 5, C.F. 00389240219, pursuant to art. 58, par. 2, lett. i), and 83, par. 5, of the Regulation and 166, paragraph 2, of the Code, to pay the sum of € 84,000.00 (eighty-four 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 thirty days, an amount equal to half of the sanction imposed;

INJUNCES

to the Municipality of Bolzano:

a) to pay the sum of € 84,000.00 (eighty-four thousand), in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, according to the methods indicated in the annex, within thirty 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;

b) pursuant to art. 58, par. 2, lett. d), of the Regulation, to adopt, within sixty days from the notification of this provision, technical and organizational measures suitable to anonymize the data relating to the employee workstation detected in the web browsing logs and to delete the personal data present in the registered web browsing, updating the internal procedures most recently identified and included in the trade union agreement of 4 February 2020;

c) 1-pursuant to art. 58, par. 1, lett. a), of the Regulations, and of art. 157 of the Code, to communicate, by providing adequately documented feedback, within thirty days of notification of this provision, the initiatives it intends to undertake in relation to the provisions of letter b) above; failure to respond to a request made pursuant to art. 157 of the Code is punished with an administrative sanction, pursuant to the combined provisions of art. 83, par. 5, of the Regulation and 166 of the Code;

HAS

the publication of this provision on the website of the Guarantor pursuant to art. 166, paragraph 7, of the Code;

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.

Pursuant to art. 78 of the Regulation, of art. 152 of the Code and 10 of the legislative decree 1 September 2011, n. 150, 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, May 13, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Stanzione

THE SECRETARY GENERAL

Mattei