SEE ALSO: press release dated December 19, 2022

[doc. web no. 9833530]

Injunction order against the Lazio Region - 1 December 2022

Register of measures

no. 409 of 1 December 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, concerning the protection of natural persons with regard to the processing of personal data, as well as the free movement of such data and which repeals Directive 95/46/ CE, “General Data Protection Regulation” (hereinafter, “Regulation”);

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

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

Given the documentation in the deeds;

Given the observations made by the general secretary pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the Guarantor's office for the protection of personal data, doc. web no. 1098801;

Speaker Prof. Pasquale Stanzione;

WHEREAS

1. Introduction.

With a report submitted pursuant to art. 144 of the Code, the independent trade union Fedirets (Federation of Managers and

Managers of Territorial Bodies and Health) represented that the Lazio Region (hereinafter, the "Region"), in the face of the alleged revelation by its employees of official news, which should have remained secret, would have carried out "a check on the emails of the regional administration's lawyers asking the manager of the computer networks of the Region [...] a check on the outgoing email flows from the institutional email boxes, attributed to the lawyers of the regional lawyer [...]".

This would have been done by analyzing information such as "sender, subject and recipient of the emails sent, as well as reconnaissance and weighing of any attachments to the emails themselves" in the email boxes of "all the lawyers of the regional administration", without there being any "reasons objective for carrying out such a massive and indiscriminate control".

The control in question would, however, have been requested not by the employer, to be identified "in the Director of the Regional Directorate for "Organization and Personnel", but, informally by the Secretary General, in the absence of "any Act [or] Provision Administrative, who has authorized [the same]" and in the absence of "regulatory procedures and policies on the use of e-mail and the Internet", since no information was provided to the workers in relation to the possibility of such controls on e-mail.

From the documentation in the documents (see note prot. n. XX of the XX of the company LAZIOcrea S.p.A. - hereinafter, "LazioCrea" - which carried out the same on behalf of the Region) it emerges that "as a matter of practice, email traffic is kept for 180 days before being definitively cancelled" and that "in order to have such traffic, one does not access either the staff computers or their mailbox […] [because] when it comes to mail traffic that the system administrator can see it [refers to] surrounding data such as [...] the day, time, sender, recipient, subject and size of the email itself. Neither the content nor any attachments can be seen. The presence of attachments can be inferred (there is no certainty) of the size of the email itself".

2. The preliminary investigation.

In response to a request for information from the Authority (note prot. n. XX of the XX), the Region, with note prot. no. XX of the XX, declared, in particular, that:

"the cause of the checks carried out derives from the obligation for the Region, as Data Controller, to ensure the security of the treatments and, in the specific case, also to protect the confidentiality of the information managed by the lawyers: the personal data contained in the -mails could have been unlawfully disseminated";

"the employer initiative concerned data connected to the employment relationship and had the objective of ascertaining any unlawful behavior by the worker, of which there was reasonable suspicion and which was also harmful to the image of the

Administration. The behaviors concern the alleged disclosure by its employees, specifically lawyers belonging to the regional Attorney's office, of official news that should have remained secret. The controls were arranged, in a confidential manner, after the implementation of the behaviors themselves, in a timely manner and limited to some data, not configuring a form of surveillance of work performance. It should be noted that the content of the e-mails was not subject to processing and that the verification activities were carried out by carrying out treatments that did not exceed the purposes pursued";

"in the information on the processing of personal data for the personnel in service, published by the XX in the section of the corporate Intranet dedicated to Privacy, it is specified that "Regione Lazio reserves the right to verify, within the limits permitted by the law and contractual , the integrity of its systems (IT and telephony)"";

"The Secretary General of the Regional Council had the duty and the correlated powers necessary to carry out the checks in accordance with the provisions of art. 19 bis paragraph 2 lett. d) and h) of the "Regulations for the organization of the offices and services of the Regional Council" no. XX of the XX in force at the time of the events [...]";

"the records do not show any copy of disposition, deed or provision through which the request to the system administrator to proceed with the control was formalized";

"the control, from a technical point of view, was not carried out by the Regional Administration, but directly by the in-house company LazioCrea, to which with the framework service contract referred to in Regional Government Decree no. XX of the XX are entrusted with the "planning, implementation and management of the regional Digital Agenda strategy, including the Regional Information System". The company has been appointed data processor with DGR n. XX and specific instructions have been provided through attachment G to the DGR n. XX. It should be noted that among the same instructions there is the following provision "Should the need arise to carry out different and exceptional processing of personal data with respect to those normally carried out, LAZIOCrea must inform the Data Controller and the Data Protection Officer (DPO) of the Lazio Region .". Following a request from the Data Controller, the LazioCrea company reported on the technical methods of carrying out the control with note prot. XX of the XX […]";

"The Lazio Region has not indicated the [...] storage time [of the metadata connected to the use of e-mail] to the LazioCrea company: it must therefore be assumed that it is the result of assessments by the company itself, which, in the aforementioned note prot. XX [...] indicates that "as a matter of practice, email traffic is stored for about 180 days before being definitively cancelled";

"at the time of the events, this Region did not consider it to be subject to the obligation to draw up an impact assessment as it was not considered that there were high risks deriving from the processing, not concerning the same particular data or data referred to in art 10 [of the Regulation] (formerly sensitive or judicial) on a large scale, nor by determining a systematic evaluation of personal aspects. However, in the light of what has occurred, the need for this fulfillment is currently being assessed".

With a note of the XX (prot. n. XX), the Office, on the basis of the elements acquired, the checks carried out and the facts that emerged following the preliminary investigation, notified the Region, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation, for having implemented the processing of personal data relating to the use of e-mail by employees:

- in a manner that does not comply with the principles of "lawfulness, correctness and transparency", "limitation of conservation" and "accountability", in violation of art. 5, par. 1, lit. a) and e), and para. 2, of the Regulation;
- in the absence of a legal basis and in a manner that does not comply with the sector regulations on remote controls of workers and the collection of data irrelevant to the work activity (Articles 4 and 8 of Law No. 300/1970), in violation of the articles 5, par. 1, lit. a), 6 and 88, par. 1, of the Regulation, as well as 113 and 114 of the Code;
- failing to provide interested parties with information on the processing of personal data, in violation of articles 12 and 13 of the Regulation;
- in a manner that does not comply with the principle of "data protection by design and by default", in violation of art. 25 of the Regulation;
- failing to carry out a prior impact assessment on data protection, in violation of art. 35 of the Regulation.

With the same note, the Region was invited to produce written defenses or documents to the Guarantor or to ask to be heard by the Authority (art. 166, paragraphs 6 and 7, of the Code, as well as art. 18, paragraph 1, of the l 24 November 1981, no. 689).

With note prot. no. XX of the XX, the Region sent its defense brief, declaring, in particular, that:

“the processing is lawful as it is “necessary for the execution of a task of public interest or connected to the exercise of public powers vested in the data controller” and for the legitimate interest of the Data Controller. In fact, the regional administration carried out an ex post assessment, i.e. after the implementation of the alleged unlawful conduct, in the presence of reasonable

suspicions of unlawful conduct by some lawyers of the regional lawyers' office, consisting in the disclosure of official information to third parties subject to secrecy. It is believed that this case is extraneous to the scope of the articles 4 and 8 of the law 300/1970";

“[…] moreover […] paragraph 2 of art. 4 of law 300/1970 excludes [and] from the provisions referred to in paragraph 1 [of the l. 300/1970] the tools used by the worker to render the work performance among which, for the subjects of interest, certainly includes e-mail ";

"the information [...] published in the section of the corporate Intranet dedicated to Privacy, indicates that "Regione Lazio reserves the right to verify, within the limits permitted by law and contracts, the integrity of its systems (IT and telephony)" . It is noted that, in the opinion of the Authority, this information is not sufficiently specific, therefore it is the intention of the Administration to supplement it [...]";

"The Administration has also decided to adopt an internal disciplinary [...] which describes the checks to which employees may be subjected, which will be adequately disseminated to them. It is also represented that, with determination XX of XX of the Institutional Affairs, Personnel and Information Systems Department, the Administration has already adopted a disciplinary";

[...] for the use of ICT equipment for the personnel in service at the offices of the Regional Council, which, in chapter 8, introduces provisions relating to controls. These provisions will be harmonized with the new internal regulations on the subject of controls";

"the [Region, following the start of the investigation,] proceeded to draw up an impact assessment on the protection of personal data relating to log management [...]";

"with reference to data retention, please refer to the DPIA regarding log management [...]. A storage time of at least 6 months is considered appropriate due to the possibility for the Administration to carry out investigative actions relating, for example, to IT attacks that are not promptly detected, as well as the complexity of the managed systems. This consideration also derives from the analogy with the provisions of the provisions [of the Guarantor] "Measures and expedients prescribed to data controllers carried out with electronic instruments in relation to the attributions of the functions of system administrator - November 27, 2008" and "Regulations on the circulation of information in the field of banking and the tracing of banking transactions - 12 May 2011" [...]";

the circumstance that "the request to the system administrator to proceed with the control has not been formalized [...]

excludes [and] a monitoring treatment and even more a "systematic monitoring" treatment of the employee activity by the Administration regional [and is] to be interpreted as an isolated one-off event";

"from a logical point of view, we do not agree with the deduction that "from the circumstance that this Region asked LAZIOCrea to carry out the checks in question on such metadata, it can be deduced that it was aware of the collection of the same, which was carried out for own account and in its own exclusive interest, by the person in charge of the treatment", as only a presumption can be derived from the request, as the Company could have replied that it did not have the data or had it for a different period. In any case, the Administration, also following the assessment of the impact on the protection of personal data relating to the management of the logs [...], will provide LAZIOCrea with appropriate instructions in order to reformulate the retention times of the metadata [...]";

"the obligation to carry out a prior impact assessment on data protection exists in the presence of "a high risk for the rights and freedoms of natural persons" (art. 35 paragraph 1 of the Regulation). A risk is a scenario describing an event and its consequences, estimated in terms of severity and probability." The logs have an extremely low probability of being accessed for purposes other than those of protecting the security of computer systems and, even in the presence of a high level of severity of data disclosure, the resulting risk was estimated as medium[…] The evaluation was not conducted as at least two applicable criteria were not found [among those indicated by the European Data Protection Board in the "Guidelines on data protection impact assessment and determination of the possibility that the treatment "may present a high risk" for the purposes of regulation (EU) 2016/679"] [...] [in any case] an assessment of the impact on the protection was carried out [on a voluntary basis and after the start of the investigation] of personal data relating to log management".

During the hearing, requested pursuant to art. 166, paragraph 6, of the Code and held on the XX date (minutes prot. n. XX of the XX), the Region declared, in particular, that:

"the Lazio Region, even before receiving the complaint from the Authority, had put in place a series of measures to make workers aware of the correct methods of using IT tools (see internal regulations of the XX, to which inside there is a paragraph on the use of e-mail and on the checks that the Region reserves the right to carry out) [...]";

“regarding the lawfulness of the processing, the Lazio Region believes that there are no conditions for the application of art. 4 of law 300/1970, given the possibility for the employer, as recognized by the Court of Cassation, to carry out defensive checks to protect its assets. In fact, it is necessary to balance the interests between the workers' right to data protection and the

employer's right to protect their own interests";

"the collection of metadata relating to the use of e-mail does not pursue the purpose of monitoring the activity of workers, being instrumental only to guarantee IT security";

"the control in question did not concern the correct execution of the work activity by the employees but was aimed at ascertaining an alleged illegal conduct";

"there are valid reasons to justify the conservation of the aforementioned metadata for a period longer than seven days, in order to guarantee the security of the information systems. For example, with regard to the 2021 cyber attacks, the investigations subsequently conducted would not have been possible if the logs had not been kept for sufficiently long periods of time, at least six months. The reasons justifying these retention times are better explained in the draft impact assessment on data protection provided by the Region attached to its defense briefs";

"The Lazio Region reserves the right to provide the Authority with further elements and information, within fifteen days from the date of the hearing, regarding the current conservation of the metadata used in the context of the controls subject to the report".

Subsequently, with note prot. no. XX of the XX, the Region sent these further elements and information, declaring, in particular, that:

"with note prot. XX of the XX, acquired under regional protocol n.XX of the XX, [...] [the] Director of the Infrastructural Systems Department of the in-house company LAZIOCREA, appointed data processor pursuant to art. 28 of Regulation 2016/679, declared that "the data of the logs relating to the traffic of the emails of the users in question referring to the XX procedure of the Guarantor [...], were at the time canceled according to what is foreseen by our procedures. The maximum retention period of the logs was at the time established in 180 days after which they were automatically deleted. The copy of the aforementioned extractions is available to the Judicial Authority which made them the subject of an independent treatment having provided for their seizure on the XX date "";

"with note prot. reg. XX of the XX the lawyer [...], Attorney Coordinator of the Regional Attorney represented that "The Direr-Dirl Lazio, which adheres to the Fedirets, has considered this activity of verification on the IT flow (limited to a small number of accounts and lasting a few hours) expression of activity anti-union (although the sender, author of the undue use of institutional e-mail, was a subject who did not hold managerial roles in the Organization), likewise the lack of response from the

Institutional Affairs Department aimed at activating a discussion for the regulation of the use of accounts companies: and thus appealed to the Court with an appeal pursuant to art. 28 Law no. 300 of 1970. The Court, by decree of 6 July 2021, in the cross-examination of the parties, rejected the appeal. Direr-Dirl Lazio then filed an objection, which - with a sentence of 7 March 2022 (which is produced with the necessary omissis, keeping the other parts of the decision to irrelevant issues here and involving other subjects) [...] was rejected by the Court of Rome [...] to confirm the total groundlessness of the opposing claim";

"with reference to the review of the information relating to employees, it should be noted that, with note prot. reg. no. XX of the XX, the [...] Director of the Regional Directorate of Institutional Affairs and Personnel communicated that "[...] the Directorate is completing the analysis of the processing processes as well as the detailed activities of all the data processing operations that it operates in the performance of its institutional functions".

With the same note, the Region filed copies of the following documents: "DGR n. XX of XX: revision of the organizational model adopted by the Regional Council on the subject of personal data protection (DGR for adaptation of regulation n. XX "Regulations for the organization of the offices and services of the Regional Council")" and "determination XX of XX of the Directorate of Institutional Affairs, Personnel and Information Systems approval of the "Regulations for the assignment and use of ICT equipment for personnel in service at the offices of the Lazio Regional Council".".

3. Outcome of the preliminary investigation.

3.1 Data protection legislation.

Based on the regulations on the protection of personal data, the employer can process personal data, also relating to particular categories of data (see art. 9, paragraph 1, of the Regulation) of workers if the processing is necessary , in general, for the management of the employment relationship and to fulfill specific obligations or tasks deriving from the sector regulations (articles 6, paragraph 1, letter c), 9, par. 2, lit. b) and 4; 88 of the Regulation). Furthermore, the treatment is lawful when it is "necessary for the execution of a task of public interest or connected to the exercise of public powers vested in the data controller" (articles 6, paragraph 1, letter e), 2 and 3 of the Regulation; 2-ter of the Code, in the text prior to the amendments made by Legislative Decree 8 October 2021, no. 139, in force at the time of the events being reported).

The employer must also comply with national rules, which "include appropriate and specific measures to safeguard human dignity, the legitimate interests and the fundamental rights of the data subjects, in particular as regards the transparency of the

treatment [...] and the systems of workplace monitoring" (articles 6, paragraph 2, and 88, paragraph 2, of the Regulation). On this point the Code, confirming the system prior to the changes made by Legislative Decree 10 August 2018, n. 101, makes express reference to the national provisions of the sector which protect the dignity of people in the workplace, with particular reference to possible controls by the employer (articles 113 "Data collection and pertinence" and 114 "Guarantees regarding remote control"). As a result of this postponement, and taking into account art. 88, par. 2, of the Regulation, the observance of the articles 4 and 8 of the law no. 300/1970 and of the art. 10 of Legislative Decree no. 297/2003 (in cases where the conditions are met) constitutes a condition of lawfulness of the treatment.

These rules constitute in the internal legal system those more specific and greater guarantee provisions pursuant to art. 88 of the Regulation - for this purpose subject to specific notification by the Guarantor to the Commission (available on the page: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/ eu-countries-gdpr-specific-notifications_en.) 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, letter. d), of the Regulation (see, most recently, with regard to the public sector, provision no. 384 of 28 October 2021, web doc. no. 9722661; provision no. 190 of 13 May 2021, web doc. no. 9669974; provision no. 90 of 11 March 2021, web doc. no. 9582791, as well as the provisions referred to therein).

The data controller is, however, required to comply with data protection principles (Article 5 of the Regulation) and is responsible for implementing appropriate technical and organizational measures based on the specific risks deriving from the processing, having to be able able to demonstrate that the same is carried out in compliance with the Regulation (articles 5, paragraph 2, and 24 of the Regulation).

3.2 The processing of personal data relating to the use of e-mail by employees.

From the elements acquired during the preliminary investigation it emerged that the Region, in order to verify alleged illicit behavior by its own personnel in service at the regional lawyers' offices, in the presence of suspicion regarding the possible disclosure to third parties of news ex officio, has instructed LazioCrea, in its capacity as its data controller, to carry out a check on the metadata relating to the use of the institutional e-mail accounts by the workers in question (day, time, sender, recipient, subject and size of the email).

This data analysis and extraction operation was possible because, as confirmed in the course of the proceedings, the metadata relating to the use of the institutional e-mail accounts assigned to the employees of the Region are collected in a preventive and generalized manner, and subsequently ordinarily kept for 180 days.

3.3 Correctness and transparency towards interested parties: information on the processing of personal data.

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

In view of this obligation, the Region, in providing its employees with the information on the processing of personal data - which would have been published on the company intranet from the XX, although no copy of the same was produced - only communicated the circumstance that it " reserves the right to verify, within the limits permitted by law and contractual provisions, the integrity of its systems (IT and telephony)", while only during the investigation did it represent its intention to adopt an internal specification to inform the workers regarding the methods for carrying out the aforesaid controls in relation to the use of IT tools by employees (see note prot. n. XX of XX).

During the proceeding it then emerged that since the 20th century the Region had adopted a disciplinary for the use of ICT equipment for the personnel in service at the offices of the Regional Council, reserving itself "for organizational or security reasons [...] the right to carry out, through LAZIOcrea, sporadic and occasional checks", and in particular to "monitor the networks and Facilities [in the event of] [...] ascertainment of undue use of e-mail", also with regard to the "volume of messages exchanged, format and size of the attached files" (par. 8 of determination XX of XX of the Institutional Affairs, Personnel and Information Systems Directorate).

In the premise that in the documents there is no proof that the employees have actually been informed of the possibility of finding and consulting the specification in question on the regional intranet (see paragraph 10 of the determination, where it is stated in general terms that " approval of the Regulations is disclosed to employees via regional intranet and/or e-mail"), it should be noted that neither the original information provided to employees nor this document contain all the elements expressly required by data protection legislation - in particular the "legal basis of the processing" and the "personal data retention period" (Article 13, paragraph 1, letter c) and par. 2, lit. a), of the Regulation) - and provide them with a clear and transparent representation of the overall processing carried out, with particular regard to the collection and storage for 180

days of metadata relating to the use of e-mail (see the "Guidelines of the Guarantor by e-mail and internet" of 1 March 2007, n. 13, web doc. n. 1387522 - which, although referring to the previous regulatory framework, contain still valid principles and indications - in particular paragraphs 3.1 and 3.3).

Compliance with the obligation to provide interested parties with all the essential information elements required by the Regulation responds to the need to allow them to be fully aware of the characteristics of the same before the processing begins. This also with regard to the collection, within a framework of lawfulness, of personal data connected to work activities (cf., judgment of the European Court of Human Rights of 5 September 2017 - Appeal no. 61496/08 - Case Barbulescu v. Romania, spec. par. n. 133 and 140).

On this point, however, it should be noted that the fulfillment of the information obligations towards employees (consisting of "adequate information on the methods of use of the tools and of carrying out the checks") constitutes a specific precondition for the lawful use of the data collected through tools technology, by the employer, also for all purposes connected to the employment relationship (Article 4, paragraph 3, of Law No. 300/1970).

While acknowledging the Region's intention to prepare new regulations regarding the use of IT resources by employees and the processing which, for organizational and IT security needs, also involves the collection and storage of metadata relating to the use of e-mail by employees, it has been ascertained that the Region has not, at the time of starting the described treatment, taken steps to provide the interested parties with all the information elements required by the Regulation, having therefore acted in a manner that does not comply with the "principle of lawfulness, fairness and transparency" and in violation of articles 5, par. 1, lit. a), 12 and 13 of the Regulation.

3.4 The lawfulness of the processing: failure to comply with the regulations on remote controls.

In general, it should be noted that the issue of data processing connected to the attribution of an institutional or company e-mail account to individual employees has for some time been brought to the attention of the Authority, both with provisions of a general nature (see the " Guarantor guidelines for e-mail and internet", cit.) and with decisions on individual cases.

The content of the e-mail messages - as well as the external data of the communications and the attached files - concern forms of correspondence assisted by guarantees of secrecy also protected constitutionally (articles 2 and 15 of the Constitution), which protect the essential core of the dignity of the person and the full development of his personality in social formations. This implies that, even in the working context, there is a legitimate expectation of confidentiality in relation to the

messages subject to correspondence (see point 5.2 letter b), of the "Guarantor's guidelines for electronic mail and the Internet", cit.; v., among many, provv. 4 December 2019, no. 216, doc. web no. 9215890 and the previous ones cited therein).

The conservation of metadata relating to the use of employees' e-mail, even if on the assumption of its necessity for IT security purposes (invoked in the present case by the Region), can involve an indirect remote control of the workers' activity, which law only allows for the recurrence of organisational, production, occupational safety and protection of company assets needs, and in the presence of the procedural guarantees provided for by art. 4, paragraph 1, of the law no. 300/1970 (trade union agreement or, alternatively, public authorisation).

Although the management of external data relating to the use of e-mail systems, contained in the so-called "envelope" of the message, and their conservation for a limited period of time, usually not exceeding seven days, can be considered necessary to ensure the correct functioning and regular use of the e-mail system, including the essential IT security guarantees (see provv.ti n. 303 of 13 July 2016, web doc. n. 5408460, confirmed by the Court of Chieti with sentence n. 672 of 24 October 2019; 1 February 2018, no. 53, web doc. no. 8159221; 29 October 2020, no. 214, web doc. no. 9518890; 29 September 2021, no. 353, web doc. no. 9719914), the conservation of such metadata, for a longer period of time, cannot, on the other hand, fall within the scope of application of art. 4, paragraph 2, of the aforementioned law. no. 300/1970. In fact, by express choice of the legislator, only the pre-ordered tools, also due to the technical configuration characteristics, for the "registration of accesses and attendance" and for the "performance of the service" are not subject to the limits and guarantees referred to in the first paragraph , as functional to allow the fulfillment of the obligations that derive directly from the employment contract, that is, the presence on duty and the execution of the work performance.

In this context, the generalized collection and storage, for a longer period (compared to the aforementioned 7 days), of the metadata relating to the use of e-mail by employees cannot, however, be brought within the scope of application of the paragraph 2 of the art. 4 of law no. 300/1970, falling, rather, among the functional tools for the protection of the integrity of the information assets of the owner as a whole, referred to in paragraph 1 of the same art. 4.

With regard to the present case, this is also proven by the fact that in the aforementioned specification of the XX the Region has reserved the right to process the aforementioned metadata - keeping them, as mentioned, for an extended period of time - "for organizational and safety" (see par. 8 of resolution XX, cit.).

Therefore, since the Region has not implemented the guarantee procedures pursuant to art. 4, paragraph 1, of the law no.

300/1970, before initiating the preventive and systematic collection of metadata relating to the use of e-mail by employees, and their conservation for a large period of time, the treatment in question appears to be in contrast with the legislation in on the protection of personal data and with the sector regulations on remote controls, in violation of articles 5, par. 1, lit. a), 6 and 88, par. 1, of the Regulation, as well as 114 of the Code (in relation to art. 4, paragraph 1, of the law n. 300/1970).

Nor can the pursuit of a legitimate interest of the data controller be invoked, for the purposes of the lawfulness of the overall processing, as proposed by the Region in its defense brief, since the same cannot be applied "to the processing of data carried out by public authorities" (see Article 6, paragraph 1, letter f), of the Regulation), and more generally, since, as specified above and constantly reaffirmed in the provisions of the Guarantor on the subject, the treatments resulting from the use of technological tools in the workplace, from which an indirect control over the working activity may derive, find their legal basis in the sector discipline referred to in art. 4 of law no. 300/1970. In fact, this provision perimeters, in a uniform way at national level, the scope of the treatment allowed in every working context (public and private) and constitutes in the internal legal system a more specific and more guarantee provision pursuant to art. 88 of the Regulation, compliance with which is a condition of lawfulness of the processing (art. 5, par.1, letter a) and 6, par. 1, lit. c) of the Regulation; see also the jurisprudence of the European Court of Human Rights, in the case Antovic and Mirković v. Montenegro, application no. 70838/13 of 11.28.2017, 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 by the applicable national law).

With regard to the compatibility with the principles of data protection of the extended retention period of such metadata identified by the Region (180 days), see the following par. 3.7.

3.5. The checks carried out on the e-mail accounts of some employees.

As can be seen from the evidence in the records, the personal data relating to e-mail messages, collected and stored in the manner described above, were then processed by the Region also for the purpose of carrying out punctual checks on specific employees.

In this regard, the defensive thesis put forward by the Region cannot be accepted, according to which it would have carried out "an ex post assessment, or after the implementation of the alleged unlawful conduct, in the presence of reasonable suspicions of unlawful conduct by some lawyers of the regional lawyers' office, consisting in the disclosure to third parties of official

information subject to the obligation of secrecy", on the assumption that "this case is extraneous to the field of application of articles 4 and 8 of the law 300/1970".

Given that the so-called theory on defensive controls, of pure jurisprudential creation, is the subject of non-univocal applications (see provision no. 137 of 15 April 2021, web doc. no. 9670738) and is based on factual circumstances that in any case do not occur in the case in point, the following should be reiterated for the data protection profiles. The processing of personal data connected to the use of tools from which the possibility of remote control of the workers' activity may also derive must be carried out in strict compliance with the limits and conditions set by the reference legislative framework, which constitutes, as said, the legal basis (articles 5, paragraph 1, letter a), 6, 88, par. 1, of the Regulation, as well as 114 of the Code, with reference to art. 4 of law no. 300/1970). This, even more so, since, following the changes made to the art. 4 of law no. 300/1970 by Legislative Decree 14 September 2015, n. 151, the need to protect the employer's assets have also been expressly included among the only lawful purposes that can be pursued through systems that can involve indirect control over the generality of employees, subordinating their installation and use to the union agreement or, alternatively, to public authorization (see the previous par. 3.4). It follows that, if these conditions are not respected for the lawful use of the aforementioned systems, any treatment, even further, of such data, including their "extraction, consultation and use" (Article 4, paragraph 1, no. 1), of the Regulation), must be considered without a suitable legal basis and therefore illegal.

Consequently, the forms of control over the activity of the workers, put in place in the absence of the aforementioned guarantees, are placed outside the framework of lawfulness outlined by the provisions of the sector and by the legislation on data protection. It should also be considered that the aforementioned sector regulations allow the use, for further purposes in the context of managing the relationship, only of the information already lawfully collected in compliance with the conditions and limits established by art. 4 of law no. 300/1970 and, therefore, within the limits in which the original collection was lawfully carried out (see provv.ti 28 October 2021, n. 384, web doc. n. 9722661, and 13 May 2021, n. 190, doc. web no. 9669974).

In the light of the foregoing considerations, the processing of personal data, consisting in the consultation of the collected metadata and in the extraction of some case studies relating to individual workers, was also carried out in violation of articles 5, par. 1, lit. a), 6 and 88, par. 1, of the Regulation, as well as 114 of the Code (in relation to art. 4, paragraph 1, of law n. 300/1970).

3.6. The collection of data not related to the work activity.

Since 1970, public and private employers have been prohibited from "carrying out inquiries, even through third parties, on the worker's political, religious or trade union opinions, as well as on facts that are not relevant for the purpose of assessing the professional aptitude of the worker" (see art. 8 of law n. 300/1970 and art. 10 of legislative decree n. 276 of 10 September 2003, expressly referred to in art. 113 of the Code).

The generalized collection and storage of metadata relating to the use of e-mail by employees, for an extended period of time, moreover in the absence of suitable legal conditions and clear indications and information given to workers (see the previous par. 3.1), also entails the possibility for the employer to acquire, during the course of the employment relationship, information on the worker's private life or on facts that are in any case irrelevant for the purpose of assessing the worker's professional aptitude.

In this regard, it should be noted that from the elements that can be obtained from the external data of the correspondence, such as the subject, the sender and the recipient and other information that accompany the data in transit, defining temporal profiles (such as the date and time of sending /reception), as well as from the qualitative-quantitative aspects also in relation to the recipients and the frequency of contact (since these data too are, in turn, susceptible to aggregation, processing and control), it is possible to acquire elements referring to the personal sphere or to the opinions of the interested party, where such information, as in the present case, is kept for particularly extended periods.

As proof of this, there is the fact that this extensive and prolonged collection made it possible to carry out the aforementioned checks and, within the context of these, a precise selection of the specific accounts to be investigated, also on the basis of other information already available and data personal data, however known, referring to the interested parties. In particular, the flows of outgoing emails from the email accounts of the staff of the regional lawyers were examined and, in particular, the messages addressed to representatives of a specific trade union (to which many workers of the lawyers had joined or with whom they were associated or sympathizers), as well as those sent to a colleague known to be a supporter of this trade union acronym (see complaint from the Region to the Provincial Headquarters of the Guardia di Finanza, in the file).

Nor can it be considered sufficient, to this end, that the employer, as in the present case, limits itself to referring to the correct use of e-mail by its employees for institutional purposes only or connected to the employment relationship, leveraging exclusively on the responsibility of employees and on the prohibition of the use of IT tools for personal purposes (see provision no. 190 of 13 May 2021, web doc. no. 9669974, par. 3.4). This is because, considering that the dividing line between the

working and professional sphere and the strictly private one cannot always be drawn clearly, the complete annulment of any expectation of confidentiality of the data subject in the workplace cannot be foreseen, even in cases in which the employee is connected to the network services made available by the employer or uses a company resource, which is why the European Court of Human Rights has confirmed over time that the protection of private life also extends to workplace, where the relations of the person who works take place (see judgments Niemietz v. Allemagne, 12.16.1992, application no. 13710/88, spec. par. 29; Copland v. UK, 04.03.2007, application . No. 62617/00, spec. para. 41; Bărbulescu v. Romania, cit., spec. para. 70-73 and 80; Antović and Mirković v. Montenegro, cit., spec. para. 41-42).

For these reasons, the conduct of the Region is also in contrast with the national provisions which prohibit the employer from acquiring (and in any case "processing") information that "[are] not relevant for the purposes of assessing the professional aptitude of the worker" or in any case relating to the private sphere of the interested parties, in violation of articles 5, par. 1, lit. a), 6 and 88, par. 1, of the Regulation, as well as 113 of the Code (in relation to articles 8 of the law n. 300/1970 and 10 of the legislative decree n. 276/2003).

3.7 Restriction of retention and data protection by design and by default.

According to the principle of "retention limitation", personal data must be "kept in a form that allows the identification of the interested parties for a period of time not exceeding the achievement of the purposes for which they are processed" (Article 5, paragraph 1, letter e), of the Regulation).

In consideration of the risk looming over the rights and freedoms of data subjects, the data controller must - "from the planning stage" and "by default" (art. 25 of the Regulation) - adopt adequate technical and organizational measures to implement the principles of data protection, integrating the necessary guarantees in the processing to meet the requirements of the Regulation and protect the rights and freedoms of data subjects (see "Guidelines 4/2019 on article 25 - Data protection from design and by default" , adopted by the European Data Protection Board on 20 October 2020, spec. points 42, 44 and 49).

This obligation "applies [also] for [...] the retention period [...]" of the data (Article 25, paragraph 2, of the Regulation).

In the present case, following the investigation, it emerged that the Region keeps the metadata relating to the use of e-mail, for general information security purposes, for a period of 180 days, which, also in the light of the provisions adopted on the subject by the Guarantor, was not justified for the pursuit of the aforementioned purposes. This is because, where necessary, any security incidents can and must be promptly detected and mitigated, to protect the integrity and proper functioning of the IT

systems, implementing the appropriate countermeasures and, if necessary, making use of the metadata relating to the use of e-mail, in any case within much more limited time limits (see provisions of the Guarantor no. 303 of 13 July 2016, web doc. no. 5408460; 1 February 2018, no. 53, web doc. no. 8159221; 29 October 2020, n. 214, web doc. n. 9518890).

It was therefore not ensured, both when determining the means of processing and during the processing itself, that the protection of personal data was integrated into the processing from its design and by default throughout the data life cycle , "incorporating in the processing the measures and safeguards appropriate to ensure the effectiveness of the principles of data protection, the rights and freedoms of the interested parties" and making sure that "[was] carried out by default only the processing strictly necessary to achieve the specific and lawful purpose", also with regard to the data retention period, "in all phases of the planning of processing activities, including contracts, tenders, outsourcing, development, support, maintenance, testing, storage, deletion, etc." ("Guidelines 4/2019 on Article 25 - Data protection by design and by default", cit.). This has therefore led to the violation of the art. 25 of the Regulation.

Nor can it be considered relevant, for the purpose of excluding the overall responsibility of the Region in this respect, the circumstance that, as stated, the same "did not indicate the [...] conservation time [of the metadata connected to the use of e-mail] to the company LazioCrea" and that, on the other hand, the determination of this metadata retention time, equal to 180 days, would have been "the result of company evaluations".

It should, in fact, be highlighted that the data controller, as the subject on whom the decisions regarding the purposes and methods of processing the personal data of the data subjects fall, bears a "general responsibility" for the treatments put in place (cons. 74 of the Regulation ; see, among others, provision no. 43 of 10 February 2022, web doc. no. 9751498 and the previous provisions referred to therein; see also the "Guidelines 07/2020 on the concepts of data controller and manager of the processing pursuant to the GDPR", adopted by the European Data Protection Board on 7 July 2021, spec. par. 174).

Based on the principle of "accountability", the owner is, in fact, required to comply with the principles of data protection (Article 5, paragraph 1, of the Regulation) and must be able to prove it (Article 5, paragraph 2 , of the Regulation), also with regard to the adequate technical and organizational measures put in place in order to guarantee compliance with the data protection and sector regulations that may be applicable (Article 24, paragraph 1, of the Regulation) .

As recently highlighted by the Guarantor, the data controller, even when using products or services created by third parties, must verify, also with the support of the Data Protection Officer, where designated, compliance with the principles applicable to

data processing (Article 5 of the Regulation) by adopting, in compliance with the principle of accountability, the appropriate technical and organizational measures and imparting the necessary instructions to the service provider (see Articles 5, paragraph 2, 24, 25 and 32 of the Regulation; see ., with regard to specific treatments in the workplace, provisions dated 28 October 2021, n. 384, web doc. n. 9722661, and 10 June 2021, n. 235, web doc. n. 9685922; but see also provv December 17, 2020, no. 282, web doc. no. 9525337). In this perspective, the data controller must ensure, for example, that the functions that are not compatible with the purposes of the treatment or that conflict with specific sector rules established by law are deactivated, especially in the workplace, commensurating also adequately the data retention times.

From the circumstance that the Region asked LazioCrea to carry out the checks in question on such metadata, it can also be deduced that the same was aware of the collection of the same, which was carried out on its own behalf and in its own exclusive interest by the manager of the treatment.

The need and the reasons aimed at justifying this extensive conservation of the aforementioned metadata were also presented by the Region itself during the preliminary investigation, in particular during the hearing, during which the need was expressed that "in order to guarantee the security of information systems" must be kept "for sufficiently long periods of time, of at least six months", thus confirming that the choices made in this regard are attributable to the Region or in any case attributable to needs invoked by the Region in as data controller.

For these reasons, the decision to set the retention period at 180 days must in any case be attributed to the Region.

Consequently, taking into account the regulatory framework of the applicable sector, the specific processing operations consisting of the generalized collection and storage for a period of 180 days of the metadata relating to the use of e-mail by employees, are also in contrast with the principles of "limitation of data retention" as well as "protection of personal data from the design and by default", in violation of articles 5, par. 1, lit. e), and 25 of the Regulation.

3.8 The accountability principle.

Given the delicacy of the processing of personal data put in place by the Region, suitable for remotely monitoring the activity of workers and allowing the employer to also get hold of information relating to their private sphere, and taking into account that such processing , for the reasons set out above, was carried out in violation of the basic principles on data protection pursuant to art. 5, par. 1, lit. a) and e), it is believed that the Region has also acted in a manner different from the principle of "accountability", in violation of art. 5, par. 2 of the Regulation (see also art. 24 of the Regulation).

3.9 The data protection impact assessment.

Pursuant to art. 35 of the Regulation, "when a type of processing, when it provides in particular for the use of new technologies, considering the nature, object, context and purposes of the processing, may present a high risk for the rights and freedoms of the natural persons, the data controller carries out, before proceeding with the treatment, an assessment of the impact of the foreseen treatments on the protection of personal data. A single assessment can look at a set of similar treatments that have similar high risks."

In implementation of the principle of "accountability" (see art. 5, paragraph 2, and 24 of the Regulation), it is up to the controller to assess whether the treatments that are intended to be carried out may present a high risk for the rights and freedoms of natural persons - due to the technologies used and considering the nature, object, context and purposes pursued - which requires a prior assessment of the impact on the protection of personal data (see cons. 90 of the Regulation).

In the present case, the processing of metadata relating to the use of e-mail was carried out even in the absence of a preliminary impact assessment on data protection on the assumption that the processing did not present specific risks for them.

Indeed, as stated by the Region in its defense brief, the Region proceeded to draw up an impact assessment on the protection of personal data "relating to log management" only after the start of the investigation, although the document in question does not appear expressly refer to the conservation of metadata relating to the use of e-mail by employees.

Taking into account the indications also provided at European level on the point, it should be noted, however, that the treatment in question, consisting in the systematic collection of such metadata (including information relating to the sender/recipient and the subject of each e-mail), in memorization for 180 days and in the possibility of carrying out extractions, processing and checks on such metadata, involves specific risks for the rights and freedoms of the interested parties in the working context (Article 35 of the Regulation).

Both in consideration of the particular "vulnerability" of data subjects in the working context (see cons. 75 and art. 88 of the Regulation and the "Guidelines concerning the assessment of the impact 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 mention "employees") and 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" (cf. criterion 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 (cf. articles 35 and 88, paragraph 2, of the Regulation; see also provision no. 11 October 2018 467, web document no. 9058979, annex no. 1, which expressly mentions the "processing carried out in the context of the employment relationship using technological systems [...] from which derives the possibility of carrying out a remote control of the activity of the employees"; see, among others, provv. 13 May 2021, no. 190, doc. web no. 9669974, par. 3.5).

For these reasons, the processing of personal data in question was carried out by the Region in the absence of an impact assessment and therefore in violation of art. 35 of the Regulation.

4. Conclusions.

In the light of the assessments referred to above, it should be noted that the statements made by the data controller during the preliminary investigation □ the truthfulness of which may be called upon to answer pursuant to art. 168 of the Code □, although worthy of consideration, do not allow overcoming the findings notified by the Office with the act of initiation of the procedure and are insufficient to allow the closure of the present procedure, since none of the cases provided for by the 'art. 11 of the Regulation of the Guarantor n. 1/2019.

Therefore, the preliminary assessments of the Office are confirmed and the illegality of the processing of personal data carried out by the Region is noted, for having carried out the processing of personal data in question in violation of articles 5, par. 1, lit. a) and e), and para. 2, 6, 12, 13, 25, 35, 88, para. 1, of the Regulation, as well as 113 and 114 of the Code (in relation to articles 4 and 8 of the law 300/1970).

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

5. Corrective measures (Article 58, paragraph 2, letters d) and f), of the Regulation).

The art. 58, par. 2 of the Regulation gives the Guarantor the power to "order the data controller or the data processor to bring the processing into line with the provisions of this regulation, if necessary, in a specific manner and within a specific period" (letter d)), as well as to "impose a temporary or definitive limitation to the treatment, including the prohibition of treatment" (letter f).

Taking note of what emerged during the preliminary investigation and taking into account the fact that the documentation in the documents shows that the Region is still collecting and storing the metadata relating to the use of e-mail by workers for a period of 180 days, it becomes necessary, pursuant to art. 58, par. 2, lit. d) and f), of the Regulation, order the limitation of the treatment, forbidding the Region to keep such data for a period exceeding seven days from the date of their collection, in the absence of the experimentation of the guarantee procedures pursuant to art. 4, paragraph 1, of the law 300/1970, as well as order the cancellation of data already collected and currently stored in excess of the term indicated above.

Pursuant to articles 58, par. 1, lit. a), of the Regulation and 157 of the Code, the Region will also have to provide for communicating to this Authority, providing an adequately documented response, within thirty days of notification of this provision, the initiatives undertaken in order to implement the above orders pursuant to the aforementioned art. 58, par. 2, lit. f), as well as any measures put in place to ensure compliance of the treatment with the legislation on the protection of personal data.

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

The Guarantor, pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation as well as art. 166 of the Code, has the power to "impose a pecuniary administrative sanction pursuant to article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, according to the circumstances of each single case" and, in this context, "the College [of the Guarantor] adopts the injunction order, with which it also orders the application of the ancillary administrative sanction of its publication, in whole or in part, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code" (art. 16, paragraph 1, of the Guarantor's Regulation no. 1/2019).

In this regard, taking into account the art. 83, par. 3 of the Regulation, in the specific case the violation of the aforementioned provisions is subject to the application of the administrative fine provided for by art. 83, par. 5, of the Regulation.

The aforementioned pecuniary administrative sanction imposed, depending on the circumstances of each individual case, must be determined in the amount taking into due account the elements provided for by art. 83, par. 2, of the Regulation.

In relation to the aforementioned elements, both the specific nature of the treatment was considered - initiated in a way that does not comply with the sector regulations on the use of technological tools in the workplace and with the indications provided over time by the Guarantor, for the profiles of competence - both the prolonged duration of the treatment, which is, moreover,

still in progress, despite the start of the preliminary investigation and the subsequent notification of an administrative violation.

The delicacy of the data processed was also taken into consideration, since they are also suitable for revealing information irrelevant to the working context and relating to private life.

On the other hand, the fact was taken into consideration that, even if the treatment is currently in progress, the Region has in any case offered a sufficient level of cooperation during the investigation and that the previous violations committed by the Region cannot be considered specific precedents " relative to the same object" (Article 83, paragraph 2, letter i) of the Regulation) with respect to the conduct in question, which refers to treatments carried out for purposes heterogeneous to those covered by the previous provisions of the Guarantor.

Based on the aforementioned elements, evaluated as a whole, it is deemed appropriate to determine the amount of the pecuniary sanction in the amount of 100,000.00 (one hundred thousand) euros for the violation of articles 5, par. 1, lit. a) and e), and para. 2, 6, 12, 13, 25, 35, 88, para. 1, of the Regulation, as well as 113 and 114 of the Code (in relation to articles 4 and 8 of law 300/1970), as a pecuniary administrative sanction withheld, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

Taking into account that the generalized collection of personal data relating to workers is still in progress, in the absence of the conditions of lawfulness envisaged by the sector regulations, it is also believed that the ancillary sanction of 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 Regulation of the Guarantor n. 1/2019.

Finally, it should be noted that the conditions pursuant to art. 17 of Regulation no. 1/2019.

ALL THIS CONSIDERING THE GUARANTOR

declares, pursuant to art. 57, par. 1, lit. f), of the Regulation, the illegality of the treatment carried out by the Region for violation of the articles 5, par. 1, lit. a) and e), and para. 2, 6, 12, 13, 25, 35, 88, para. 1, of the Regulation, as well as 113 and 114 of the Code (in relation to articles 4 and 8 of law n. 300/1970), in the terms referred to in the justification;

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, to the Lazio Region, with registered office in Via Cristoforo Colombo, 212 - 00147 Rome (RM), Tax Code 80143490581, to pay the sum of 100,000.00 (one hundred thousand) euros as an administrative fine for the violations indicated in the justification. It is represented that the

offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the fine imposed;

ENJOYS

to the aforementioned Region:

a) to pay the sum of Euro 100,000.00 (one hundred 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 attachment, within thirty days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the law no. 689/1981;

b) pursuant to art. 58, par. 2, lit. d) and f) of the Regulation, the limitation of processing, prohibiting the Region from any further processing operation with regard to metadata relating to the use of e-mail by workers, kept for a period exceeding seven days from the date of their collection, in the absence of the guarantee procedures pursuant to art. 4, paragraph 1, of the law 300/1970, as well as the cancellation of data already collected and currently stored in excess of the term indicated above;

c) pursuant to articles 58, par. 1, lit. a), of the Regulation and 157 of the Code, to communicate to this Authority, providing an adequately documented response, within thirty days of notification of this provision, the initiatives undertaken in order to implement the above orders pursuant to the aforementioned art. 58, par. 2, lit. f), as well as any measures put in place to ensure compliance of the treatment with the legislation on the protection of personal data.

HAS

the publication of this provision on the Guarantor's website pursuant to art. 166, paragraph 7, of the Code (see art. 16 of the Guarantor's Regulation no. 1/2019);

the annotation of this provision in the internal register of the Authority, provided for by art. 57, par. 1, lit. u), of the Regulation, of the violations and of the measures adopted in accordance with art. 58, par. 2, of the Regulation (see art. 17 of the Guarantor Regulation n. 1/2019).

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

Rome, 1st December 2022

PRESIDENT

Station

THE SPEAKER

station

THE SECRETARY GENERAL

Matthew