[doc. web n. 9670738]

Order injunction against Clear Channel Italia S.p.A. - April 15, 2021

Record of measures

n. 137 of April 15, 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 (hereinafter, the "Regulation");

GIVEN the Code regarding the protection of personal data, containing provisions for the adaptation of the national system to Regulation (EU) 2016/679 (Legislative Decree 30 June 2003, n.196, as amended by Legislative Decree 10 August 2018, no. 101, hereinafter the "Code");

GIVEN the complaints submitted to the Guarantor pursuant to Article 77 of the Regulations by Dr. XX and by dr. XX towards Clear Channel Jolly Pubblicità S.p.A .;

EXAMINED the documentation in deeds;

HAVING REGARD to the observations made by the Secretary General pursuant to art. 15 of the Guarantor regulation no. 1/2000;

RAPPORTEUR prof. Pasquale Stanzione;

WHEREAS

1. Complaints against the company and the preliminary investigation.

Dr. XX and Dr. XX, with distinct complaints presented to the Authority, respectively on November 23, 2018 and December 22, 2018, complained of alleged violations of the regulations regarding the protection of personal data with particular reference to the processing carried out by Clear Channel Jolly Pubblicità S.p.A. (now called Clear Channel Italia S.p.A., hereinafter, the company) on the data contained in the company tools (smartphones and PCs) delivered to the complainants as part of the employment relationship. The complaints were processed by acquiring a copy of all the contents present in the aforementioned devices following the momentary return of the same requested by the company to a group of employees including the

complainants.

Taking into account that the two complaints were presented against the same owner, in relation to processing operations that, following the outcome of the investigation, were found to have been carried out with similar purposes and methods, as part of the same internal investigation of the group to which the company belongs, the proceedings relating to the two complaints are defined with a single provision of the Authority.

I. Complaint of 23 November 2018.

1.1. With the complaint presented by Dr. XX complains, in particular, that on 21 September 2018 some representatives of the company PricewaterhouseCoopers (PwC) represented to the complainant "that they had been entrusted, by the company Clear Channel, with copying the contents of mobile phones, laptops and fixed […] supplied, without furnishing [re] explanations ". Only after the return of the devices did the company provide some information on the examination carried out a few hours earlier on the content of the company devices (see email 21.9.2018, h. 16.27, Annex 2 complaint 23.11.2018). This examination of the devices would have been carried out in the absence of prior specific information to the interested party, who would also not have been provided with any feedback in response to the request addressed to the company to have a copy of the documents containing the company policy on the use of the devices (v. email 5.10.2018, h. 10.43, Annex 2, complaint cited).

In response to the invitation to provide feedback, formulated by the Office on 1 March 2019, the company with a note dated 5 April 2019, stated that:

to. the company “was the subject of some internal investigations by the parent company Clear Channel International aimed at ascertaining an alleged violation of tax regulations and an alleged fraudulent conduct”; in this context, the parent company “relied on external consultants including PricewaterhouseCoopers” (see note 5.4.2019, p. 1);

b. the complainant and other employees were “suspected” of having committed crimes, including of a criminal nature (see note cit., p. 1);

c. during the internal investigations "it was deemed necessary (after having made use of legal advice on data protection in Italy) to carry out a series of forensic investigations without prior notice on a selected group of company assets entrusted to suspects to verify the reasonable doubt of unlawful conduct "(see cit. note, p. 2);

d. the lack of notice was intended to "protect the legitimate interests of the company [...] to prevent and ascertain crimes as

well as to prevent the destruction of relevant material" (see note cit., p. 2);

And. with regard to the legal basis of the processing carried out, the company has considered that the articles 6, par. 1, lett. f), 9, par. 2, lett. f) and 10 of the Regulations; furthermore, the complainant is “subject to the company's corporate policy by virtue of the existing contract” with the company that has made the documents relating to the privacy policy available in a shared folder (see note cit., p. 2);

f. measures have been taken to "reduce the risk of data privacy violation" of the complainant, in particular "by limiting access to data to a small group of external parties belonging to the PwC forensic team", "by limiting search terms to those relevant solely for the purposes of the forensic investigation "," ignoring any photograph or personal email found inadvertently "," providing that PwC does not search or bypass any passwords relating to personal information contained in personal email addresses "(see note cit., p. 3);

g. the complainant "has signed a consent form for the collection of [his] material" (see cit. note, p. 4 and Doc. 4, "Chain of Custody Form");

h. during the disciplinary procedure, the company used "a chain of emails" containing emails "sent to and from the personal email addresses" of the complainant, in this regard it should be noted that "during the exchange of subsequent emails one of the recipients forwarded the message to [the complainant's] corporate email address allegedly in error. The email exchange itself was retrieved from the company email address "(see cit. Note, p. 3-4);

the. “Computer forensic research has fueled reasonable suspicion. Following the discovery of incriminating material present in these computers, [the complainant] and his conspirators were fired ”(see note cit., P. 4).

The company has also provided a copy of the "Policy on the acceptable use of information security" (dated 26.4.2018), the "Policy on the classification and management of information" (dated 26.4.2018), the document "We protect the data we use" (dated 25.5.2018), of the "Investigation Action Protocol" (undated) in English, of the CCI Policy Store-Due diligence (undated).

1.2. With a subsequent note dated 19 June 2019, the company, represented and defended by the lawyer Francesca Rubina Gaudino, in response to a request for further clarification made by the Office on 7 May 2019, further stated and specified that:

to. "In March 2018 the company undertook an internal tax audit activity in collaboration with the auditing firm PricewaterhouseCoopers (PwC)", this "following an internal report (so-called whistleblowing)" (see note 19.6.2019, p. 2);

b. as a result of this activity, during which some "anomalies attributable to potential fraud against the Italian tax authorities" had

emerged, the company had an "in-depth internal investigation", during which "some suspicious facts in relation to potential fraudulent activity in the management of a specific service by the complainant; consequently the company in September 2018 launched a further investigation phase, again in collaboration with PwC (see note cit., p. 2);

c. in this context, on 21 September 2018, the company "asked some workers to undergo an examination of their company computers and smartphones" (see note cit., p. 2);

d. as a result of this investigation, "multiple evidence proving the involvement" of the complainant in illegal activities emerged; subsequently the complainant was subjected to disciplinary proceedings which was followed, on January 31, 2019, by the termination of the existing employment relationship (see note cit., p. 2);

And. the computer assigned to the complainant was subjected to the so-called imaging "or the copying of all areas of the hard disk [...] and the consequent archiving in a separate file"; the imaging activity "was technically carried out through" Logicube forensic Falcon ""; moreover, the company SIM was “subjected to the acquisition of the file system with« Cellebrite Ufed Touch2 »” while no investigation was carried out against the “personal mobile phone of the complainant” (see note cit., p. 3);

f. “During the checks […] PwC did not perform any access to the company server” (see cit. Note, p. 3);

g. "The specific purpose for which the investigation (and the related control activity) was conducted is to ascertain the unlawful conduct committed by the complainant"; in carrying out this activity, the company “took into consideration the principle of relevance and not excess of the checks carried out on the electronic devices supplied to the worker” (see note cit., p. 3-4);

h. "The personal data collected were of a purely non-sensitive nature [...] and to the extent [...] relevant for the purposes of the investigation. Therefore, if an initial preliminary analysis of the aggregate data contained in the devices had revealed the irrelevance and the non-stringent need to examine certain information, the company and PwC would not have continued with the control of the same. Proof of this is the fact that all personal data from private email addresses or data in any case deemed unrelated to the investigation were not taken into consideration "(see note cited, p. 4);

the. "The internal investigation covered the period of time from January 2014 up to the time of the acquisition of the complainant's computer and company SIM (September 2018)" (see note cit., P. 4);

j. "All the company policies of the company [...] are placed in a specific shared folder within the company intranet to which every worker, including the complainant, has free access" (see note cit., P. 4);

k. "Each worker receives, at the time of their first access to the company computer, a communication containing [...] an

invitation to view all the policies and codes of conduct of the company, including therefore those on the correct use of information devices and the processing of personal data "(see cit. note, p. 5);

L. "The Investigation Action Protocol was drafted by the CCI parent company and shared at the group level. This document is present in the International Sharepoint and can be consulted by all the employees of the company. It identifies the main steps connected with the activation of an investigation, starting with the appointment of an "Investigation Lead" "(see note cited, p. 5);

m. "With the advent of the Regulations [the Investigation Action Protocol] was updated, which ended in May 2018. The new version of the document was included in the International Sharepoint [...]" (see cit. Note, p. 5);

n. "Other corporate documents relating to the use of corporate IT tools adopted by the Clear Channel group are [...] Safety standards for the use of the IT equipment supplied and for the processing of corporate information [and] Information classification policy" (see cit. note, p. 5);

or. "The fact that limited use is allowed for personal purposes does not in any way prejudice the possibility of carrying out control activities" (see note cit., P. 6);

p. "The company [...] has always remained transparent in highlighting, on the one hand, the absence of any expectation of privacy in the use of company IT resources [...] and, on the other, the legitimacy of the control carried out for the detection of unlawful conduct "(see cit. note, p. 6);

q. "CCI, as the parent company, played a role of initiative and coordination of the internal investigation activity. Considering the nature and central position of CCI within the corporate structure, the legitimate interest (Article 6, paragraph 1, letter f) of the Regulation) on which it based its personal data processing activity is deduced. […] In the management of the defensive controls object of the complaint ”(see cit. Note, p. 6);

r. "The two companies [have] moved to carry out all those actions aimed at exercising and / or defending a right before an administrative and / or judicial authority, in accordance with art. 9, par. 2, lett. f) of the Regulations "(see cit. note, p. 6);

s. “No data relating to criminal convictions and offenses was analyzed during the defensive control operations” (see note cit., P. 7);

t. "The company, supported by the prevailing jurisprudential orientation, believes that the defensive control put in place against the complainant is beyond the applicability of the provisions of art. 4 Stat. Work " (see note cit., p. 7).

The company has also provided a copy of the Security Standards for the use of the IT equipment supplied and for the processing of company information (dated February 2018) and the Compliance Memo on the privacy impact assessment (dated 15.9.2019, translation into Italian) .

1.3. With a subsequent note dated January 24, 2020, provided in response to a request for further clarifications dated October 1, 2019, sent back on January 10, 2020, the company stated that:

to. the parent company Clear Channel International has adopted an internal reporting system "for itself and all affiliated companies", through the adoption of the Protected Disclosure (Whistleblowing) Policy, and "has prepared an adequate privacy policy [...]. (see note 24.1.2020, p. 2);

b. "It should be noted that the imaging operations carried out against the complainant became necessary following the findings that emerged from the first investigative phase [...] and not from an internal report" (see note cit., P. 2);

c. "The Pwc company carried out the investigations as a forensic investigator on the basis of the contractual commitment assumed [on] 24 April 2018 [...] and subsequently amended in September 2018 to extend the subject of the investigation" (see note cit ., p. 3);

d. the company had "duly instructed Pwc on the need to collect only the information strictly relevant to the case in question and to exclude (or in any case delete securely if incorrectly collected) anything that was not relevant, including data of a sensitive nature" (see . cit. note, p. 3).

Attached to the note of 8 November 2019, copies of the following documents were provided:

Protected Disclosure (Whistleblowing) Policy (dated 1.5.2019, Annex 1, English language);

FAQs relating to the Protected Disclosure (Whistleblowing) Policy (undated, Annex 2, English language);

Privacy policy relating to the whistleblowing system (undated, Annex 3, English language);

Copy of the contract signed with PwC (dated 24.4.2018, Annex 4, English language);

Amendment to the contract signed with Pwc (undated, Annex 5, English language).

II. Complaint of 22 December 2018.

1.1. With the complaint presented to the Authority, Dr. XX complains of having learned with a note dated 27 June 2018 (containing a disciplinary dispute) that the company "in the months between March and June 2018 [had conducted] an in-depth tax audit - subsequently extended to a real internal investigation - with the 'help from the PwC auditing company ". This activity

would have been carried out by accessing the contents of the mobile phone and the company laptop, delivered by the complainant himself on 24 April 2018 at the request of the company that defined the verification on the devices "as a routine part of the tax verification" (see complaint cit., p. 2 and Annex 5).

This examination of the devices, according to the complaints, would have been carried out in the absence of prior specific information to the interested party, given that the document provided at the time by the company would not contain any reference to the correct use of the work tools "while on the methods and purposes of any checks, consent is even requested to carry out audits […] "(see complaint cited, p. 3 and Annex 8). The company would also have published on the company intranet ("without any information to the worker or training") the document "Safety standards for the use of the computer equipment supplied and for the processing of company information", dated on the January title page 2008 in which, with reference to "the use of the e-mail and internet account [...] it is specified that the company reserves the constant power of monitoring", in violation of the provisions and principles of data protection (see complaint cit., p. 3-4 and Annex 9).

Finally, it was complained that the company would not have provided a response to the request to "have detailed evidence of the management of [...] personal data from the beginning of the [...] [employment] relationship", made by the complainant with an email dated 3.9.2018 (see complaint cited, p. 6-7 and Annex 10).

1.2. The company, represented and defended by the lawyer Francesca Rubina Gaudino, in response to the request for elements formulated by the Office (on March 29, 2019), in a note dated May 22, 2019 stated that:

to. "On the initiative of the parent company Clear Channel International LTD", "an internal investigation [...] about some complex commercial transactions" was started (see note cited, p. 1);

b. "In March 2018 the company undertook an internal tax audit in collaboration with the auditing firm PricewaterhouseCoopers (PwC)", this "following an internal report (so-called whistleblowing)" (see note cit., P . 2);

c. "During this activity [...], on 24 April 2018 the company asked the members of the management team to undergo an examination of their company laptop and smartphone"; subsequently “the company considered […] it necessary to launch an in-depth internal investigation” (see cit. note, p. 2);

d. "The investigations which are the subject of the disputed complaint were carried out in order to ascertain unlawful conduct that has nothing to do with the correct performance of the work [...]" (see note cit., P. 3);

And. "As for the methods of carrying out the control activity by the company, the company laptop and smartphone assigned to

the complainant were subjected to the so-called imaging, ie the copy of all areas of the hard disk of the examined device and the consequent archiving in a separate file "(see cit. note, p. 4);

f. "The complainant was notified in advance of the planned imaging activity [...]" (see note cit., P. 4);

g. "As an employee of the company, the complainant received, at the time of hiring and subsequently updated over time, information on the processing of personal data" (see note cited, p. 5 and Annex 4);

h. within the aforementioned information "among the various purposes indicated, in this case it is relevant not only that relating to the audit activity [...], but rather to the processing of data with regard to disputes and / or disciplinary proceedings" (see cit. note, p. 6);

the. "The purpose of the audit services for which the consent of the interested party was requested (and obtained) was intended to resume the provisions of letter b) [of par. 7 of the Guidelines for e-mail and Internet of the Guarantor, 2007] which requires that the processing of data not legitimized by legal and / or contractual obligations, or by legitimate interest or the exercise of rights in court, can only be based on the prior consent of the interested party "(see cit. note, p. 6);

j. the company has also produced copies of additional information documents: "Security standards for the use of the IT equipment supplied and for the processing of company information", "Policy on the classification of information" and "Policy on the acceptable use of security informatics"; within these documents "the company has clearly stated that the use of company devices must be aimed at professional purposes. The fact that limited use is allowed for personal purposes does not in any way affect the possibility of carrying out control activities […] "(see cit. Note, p. 7 and All. 5-6-7);

k. "The company therefore has always remained transparent in highlighting, on the one hand, the absence of any expectation of privacy in the use of corporate IT resources [...] and, on the other, the legitimacy of the control carried out for the detection of conduct illicit "(see cit. note, p. 7);

L. the information documents referred to above (see previous letter j.) "are placed in a specific folder shared within the company intranet to which every employee, including the complainant, has free access" (see note cit., p . 8);

m. the PwC auditing firm "complied with [the] terms of service [...] signed with the company, which contain specific provisions on the management of personal data [as well as] the instructions of the company, which expressly requested [...] to manage the revision operations in accordance with search parameters aimed exclusively at the [concrete] case and not to take into consideration and eliminate as soon as possible all the not strictly relevant information that may have emerged during this

research. […] ”(See cit. Note, p. 8);

n. with reference to the request submitted by the complainant on 3 September 2018, the company stated that "pursuant to and for the purposes of art. 15 of the Regulation [...], the data controller is not required to provide information concerning the ways in which the personal data of the interested party are processed [...]. The company therefore considered that it was not required to accept the complainant's request […]. Secondly, [...] such a communication could seriously compromise the proper conduct of the defensive investigations and the subsequent exercise of a right in court. Also for this reason, therefore, the company has decided not to provide a reasoned response to the complainant for the time being in compliance with the provisions of art. 2-undecies, c. 3, of the [Code] "(see cit. Note, p. 9).

The company also provided a copy of the "Investigation Action Protocol - Clear Channel International - Internal Audit and International Compliance", containing the protocol "in which the main steps deriving from the activation of an [internal] investigation are identified", dated November 2016 (see cit. Note, p. 7 and Annex 8; this document is also present on the intranet and only in English).

1.3. With a subsequent note of 8 November 2019, providing feedback to the request for further clarifications made by the Authority on 1 October 2019, the company further stated that:

to. “The parent company Clear Channel International […] has equipped itself with an internal reporting service for itself and all affiliated companies […]”; "The content of the documentation in question is available to all staff [...] who can view it at any time in the shared folder on the company server" (see note 11.8.2019, p. 2);

b. in accordance with the provisions of the Protected Disclosure Whistleblowing Policy "if [...] it is intended to proceed with an internal investigation following a report, all the measures described in the Investigation Action Protocol and the applicable national law will be taken into consideration" (see cit. note, p. 2);

c. with reference to the need to carry out a privacy impact assessment in the specific case pursuant to art. 35 of the Regulation, the company believes that "the imaging operations and subsequent access to the information collected in relation to the complainant [...] were carried out in a period prior to the entry into force of the Regulation" (see note cit., P . 2);

d. "CCI, as the parent company, played a role of initiative and coordination of the internal investigation activity. Considering the nature and central position of CCI within the corporate structure, the legitimate interest (Article 6, paragraph 1, letter f) of the Regulation) on which it based its personal data processing activity is deduced. "(See cit. Note, p. 2-3);

And. "The two companies [have] moved to carry out all those actions aimed at exercising and / or defending a right before an administrative and / or judicial authority, in accordance with art. 9, par. 2, lett. f), of the Regulations "(see cit. note, p. 3);

f. the PwC company operated on the basis of a contract in which "the criteria to be followed in carrying out the investigative activity are specified"; in this regard, moreover, "CCI had duly instructed PwC on the need to collect only the strictly relevant information [...] and to exclude (or in any case delete securely if incorrectly collected) all that was not relevant, including data of a sensitive nature" (see . cit. note, p. 3);

g. the data referring to the complainant "collected during the investigation operations relate to the information present on the desktop of the complainant's laptop and on Microsoft's SourceOne and Outlook365 platforms" (see cit. note, p. 3-4);

h. "The internal investigation covered the period of time from the beginning of 2016 to the time of the acquisition of the complainant's laptop and company SIM (April 24, 2018). This temporal depth was considered reasonably necessary to be able to examine any preliminary activities with respect to the suspicious transactions under investigation "(see note cit., P. 4);

the. "No data taken from the use of company tools entrusted to the complainant have been stored on the company server" (see note cit., P. 4);

j. "The company [...] believes that the defensive control put in place against the complainant is beyond the applicability of the provisions of art. 4, Stat. Work " (see cit. note, p. 4).

Attached to the note of 8 November 2019, copies of the following documents were provided:

Protected Disclosure (Whistleblowing) Policy (dated May 1, 2019, Annex 1, English language);

FAQs relating to the Protected Disclosure (Whistleblowing) Policy (Annex 2, English language);

Privacy policy relating to the whistleblowing system (Annex 3, English language);

Copy of the contract signed with PwC (dated 24 April 2018, Annex 4, English language).

2. Start of the procedure for the adoption of corrective measures.

2.1. On 10 March 2020, the Office notified the company, pursuant to art. 166, paragraph 5, of the Code, the alleged violations found, with reference, as regards the complaint of 23 November 2018, to articles. 5, par. 1, lett. a) and c) (principles of lawfulness, correctness and minimization), 6 (legal basis of the processing), 12 (information, communications and transparent methods for exercising the rights of the data subject), 13 (information) and 88 (more specifications at national level) of the Regulation; 113 (data collection and relevance) and 114 (guarantees regarding remote control) of the Code; with regard to the

complaint of 22 December 2018, in articles 11, paragraph 1, lett. a) and 13 of the Code, text in force at the time of the facts (the relevant cases are merged into articles 5, paragraph 1, letter a) and 13 of the Regulation) (principle of lawfulness and correctness and information), and articles . 5, par. 1, lett. c) (principle of minimization), 6 (legal basis of processing), 12, par. 3 and 4 in relation to art. 15 of the Regulation (transparent communications and methods for exercising the rights of the data subject), 88 (more specific provisions at national level) of the Regulation; articles 113 (data collection and relevance) and 114 (guarantees regarding remote control) of the Code.

With defense briefs of June 15, 2020, substantially identical in content relating to the cases in point of complaint except for some differential elements which will be accounted for in subsequent letters (d. And e.), The company, represented and defended by lawyers Rocco Panetta and Federico Sartore , stated that:

to. on the occasion of "the entry into force of the GDPR, the Company and the Group to which it belongs considered it essential to invest significant resources, both human and economic, in an adaptation and verification project of the entire Privacy & Data Protection setting of the Group"; in this regard, "in-depth revision and audit activities were carried out on the documentation and processes in place, as well as the reorganization, rationalization and storage of documentary data flows"; in addition, the company has set up a centralized privacy office, an Information Security Team and specific "data Champions" at the local level, and has also carried out "numerous training and education sessions for all staff" (see notes June 15, 2020, p . 2);

b. in any case "we highlight the desire and constant activity of the Group to improve its practices, flows and processes of data processing, also and above all with respect to the peculiarities of the individual national legal systems" (see notes June 15, 2020, p. 3);

c. "The forensic investigation activity that involved the devices [of the complainants] cannot and must not be considered a" mere "control activity by the employer", as it is an "absolutely extraordinary investigative activity compared to normal company activities and intended […] to investigate the alleged offenses committed with the greatest possible attention, as well as to defend one's rights in (pre) litigation ”(see cit. notes, p. 4);

d. following the receipt of a "whistleblowing" from reliable sources, together with circumstantial evidence, of alleged illegal conduct "of the complainant (with regard to the facts covered by the complaint of 22 December 2018) and, subsequently, to the outcome of an initial investigation phase during which "some suspicious facts in relation to potential fraudulent activities"

emerged (relating to the facts covered by the complaint of 23 November 2018), the company "instructed an external party, PriceWaterhouseCoopers [...] to carry out forensic investigation activities on devices […] this for the purposes of the then current «Code of ethics and good conduct for the processing of personal data carried out to carry out defensive investigations» "; in this context "the right to be informed about the methods and purposes of the processing [...] must necessarily find a form of attenuated application (even excluded), under penalty of serious and possibly irreparable damage to the party's right of defense" (see cit. notes, respectively p. 5 and p. 4.5);

And. otherwise, "even by including the imaging and analysis of the devices of [the complainants] within the perimeter of standard employer controls [...] it is believed that the corpus of information globally provided to the interested party satisfies the transparency obligations of the company" , taking into account the content of the information on data processing issued at the time of hiring to one of the complainants, the Security Standards and the Investigation Action Protocol, available in the shared folder; in addition to the information contained in the aforementioned documents, as regards the facts covered by the complaint of 22 December 2018, the "communication sent by the Company the day before the collection of the devices for carrying out the imaging activity", as regards the facts object of complaint of 23 November 2018, the "communication sent by the company on the day of collection of the devices for carrying out the imaging activity" (see cit. notes, p. 6-7);

f. with reference to the alleged violation of the principles of minimization and proportionality of the control activities prefigured by the company in the corporate documents placed on the intranet, the company "if on the one hand [...] admits the existence of a certain degree of improvement of the documentation - assuming at the same time, the solemn commitment to fill any possible difference in height - on the other hand, it is firm in deeming unfounded [...] the passage made by the Authority from the "virtual" infringement of the principles of minimization and proportionality [...] to the challenge of a pecuniary administrative sanction that 'legal system is linked to the actual violation of the same principles "(see cit. notes, p. 9);

g. the company "in a collaborative perspective of full accountability, undertakes to promptly review and correct the methods and content of the information provided to the interested parties regarding the controls that may be lawfully carried out on the IT tools made available" (see notes cit ., p. 10);

h. in order to carry out the "forensic investigations", the company "provided the consultant [...] PwC with a detailed list of keywords (so-called keywords) so that the visibility of the content of the devices was limited to what is strictly necessary to demonstrate the involvement of [the complainants] in illegal transactions "; moreover, “no strictly personal content [of the

complainants] was analyzed by PwC" (see cit. notes, p. 10);

the. "Shared the importance of translating the relevant policies in terms of disclosure requirements into Italian, it is also important to underline the complexity of the international group contexts such as the one in which the company operates" (see cit. Notes, p. 10);

j. "The processing of the data of [the complainants] and the strictly connected communication of infra-group data within the European Union [took place in the presence and on the basis of the more than solid legitimate interest consisting in the protection of interests and rights of the Company in court (and in the pre-litigation phases) "(see cited notes, respectively p. 12-13 and 12);

k. "Considering the fact that access was made only through the rigorous filter of keywords, the forced assimilation that was carried out between forensic investigation and monitoring of work activity is not understood" (see cit. Notes, p. 14) ;;

L. "The facts under analysis took place within the so-called grace period provided for by art. 22, paragraph 13 of the legislative decree n. 101 of 10 August 2018 "(see cit. Notes, respectively p. 15 and p. 14).

2.2. On July 16, 2020, the Authority held a hearing relating to the two complaints at the request of the party, during which the company, in reiterating its positions, represented that the group to which it belongs "is characterized by the classic English-centric multinational structure. In this context, there is traditionally a different sensitivity between the processing of data in the commercial sphere and that relating to employee data. [...] The company does not carry out a systematic monitoring of employees, as envisaged in the notification of violations by the Office, but has operated, in this case, through defensive checks and investigations in the presence of specific concrete circumstances vis-à-vis the complainants ". With a subsequent note received on 31 July 2020, the company provided an updated overview of the proceedings pending before the competent authorities, initiated against the complainants. Finally, with a note dated March 3, 2021, the company sent to the Authority a copy of the sentence of the Court of Padua, section, work, February 25, 2021, which rejected the appeal presented by one of the complainants concerning the request for nullity of the company's withdrawal from the collaboration relationship with the interested party, considering the retaliatory nature of the withdrawal itself not proven.

3. The outcome of the investigation and the procedure for the adoption of corrective and sanctioning measures.

3.1. Upon examination of the declarations made to the Authority during the procedure as well as of the documentation acquired, the complaints are justified for some profiles, as the company, as owner, has carried out processing operations of

personal data that are not comply with the regulations on the protection of personal data in the terms described below.
Given that, unless the fact constitutes a more serious offense, whoever, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces false acts or documents, is liable pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor", on the merits it emerged that Clear Channel Italia S.p.A. (formerly Clear Channel Jolly Pubblicità S.p.A.) carried out an internal investigation into the complainants, on the initiative of the parent company Clear Channel International LTD and following receipt of an internal report, availing itself of the auditing firm PricewaterhouseCoopers (PwC). In particular, on 23 April 2018, the Head of Data Privacy of the parent company communicated via email to one of the complainants and other subjects (members of the management team, see point 1.2., Letter c) that the following day, as part of a routine internal tax investigation, they should have delivered their corporate devices (laptops and smartphones) to PwC who would return them as soon as possible. In the face of some doubts expressed by the complainant the day after the delivery of the aforementioned devices, the same Head of the confidentiality of the parent company specified that the control activity would be limited to the information relating to a specific project and that in any case the legal basis of the processing carried out consisted in the legitimate interest of the company (parent company) in preparing a possible defense against any tax disputes (see note 22.5.2019, Doc. 5 and 6). The depth of the investigation carried out backwards, by examining the data acquired through the so-called device imaging, was, according to what was declared, equal to approximately two years and four months (from the beginning of 2016 to April 24, 2018). At a later time (September 2018) a further group of employees, including the second complainant, was subjected to imaging of the corporate devices entrusted to them, following the emergence of "suspicious facts" also regarding their work. In this case, the depth of the investigation was wider (about four years and eight months).
However, it does not appear that the complainants have been previously informed by the company about the possibility for the latter to investigate the content stored on company devices (PCs and smartphones) after subjecting them to imaging.
In particular, the information issued at the time of recruitment to one of the complainants (see with reference to the complaint of 22 December 2018, note of the company 22.5.2019, Annex 4) refers to the possibility of communicating personal data to third parties in the scope of generic audit activities as well as for the purpose of "managing any disputes and disciplinary proceedings", without any specific indication of the control methods that the data controller reserves the right to carry out on company devices. There is no copy of an individual disclosure issued to the second complainant.

As regards the documents "Safety standards for the use of the IT equipment supplied and for the processing of company information" and "Investigation Action Protocol", which also contain references - with different levels of specification - to the carrying out of checks on email, Internet browsing and telephone communications from employees, the company limited itself to placing them in a shared folder. No evidence was produced that this documentation was effectively and adequately made known to all employees (including complainants), for example through notifications (including via email) containing an invitation to become aware of it, at the time of adoption and / or on the occasion of their eventual updating. The adequate and effective publication of documents relating to the possibility of carrying out such checks is all the more necessary, in application of the principles of transparency and correctness on the part of the employer, the more the degree of control envisaged is profound and intrusive (see, further on, par. 3.3.).

Furthermore, and in any case, it is noted that the formulations used in the aforementioned documents, in referring in general terms to "monitoring" activities, are not suitable for clearly representing the purposes and specific methods of the proposed controls to the interested parties, and therefore the concrete hypotheses in which the employer "reserves the right to carry out checks in accordance with the law, indicating the legitimate reasons - specific and not generic for which they would be carried out and the relative methods" (see "Guidelines by e-mail and internet", provision no. 13 of 1 March 2007, (Official Gazette 10.3.2007, no. 58).

It is also noted that the documents "Protect the data we use" (25.5.2018), "Policy on the acceptable use of information security" (26.4.2018) and "Protected Disclosure (Whistleblowing) Policy" (1 .5.2019), provided to the Authority during the investigation, have a date subsequent to the fact that is the subject of the complaint of 22 December 2018. The document relating to the discipline of the so-called whistleblowing also follows the facts that are the subject of the second complaint, which, however, according to what has been declared, do not originate directly from an internal report. In any case, and with particular reference to the facts covered by the complaint of 23 November 2018, this documentation is, also in this case, made available to employees and the complainant exclusively by mere insertion in a shared folder, without this sharing being been adequately highlighted to the interested parties through simple tools abstractly available (eg alerts or notifications). On this point it is reiterated that, contrary to what the company believed, the depth of the investigation and the specific control methods carried out were not predictable in light of the information provided by the company on this point.

Finally, the email sent by the data privacy manager of the parent company on 23 April 2018 (at 11.53 pm) is not suitable for

providing the information required by the legal system, announcing to the interested parties, with very short notice, the withdrawal of PCs and smartphone, however, noting that these would have been purely routine checks, without referring to the imaging activity (facts covered by the complaint of 22 December 2018) nor, even less, can the communication made in the afternoon of the same day be considered suitable for this purpose. which had already been requested to return the devices (facts covered by the complaint of 23 November 2018).

With reference to the claims made by the company in the defense briefs, it is also noted that the attenuation of the information obligations placed on the data controller, in order not to nullify the right of defense of the latter, does not affect the obligation of owner to indicate, in advance and in a transparent manner, the control activities that can be carried out; 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 (on the general obligation to provide prior information about the procedures for carrying out checks in the workplace see ECHR, Bărbulescu v. Romania [GC], 5.9.2017 (rec. no. 61496/08), para. 133; López Ribalda and others v. Spain, 9.1.2018 (ric. . n. 1874/13 and 8567/13), para. 115; see also, on this point, Recommendation CM / Rec (2015) 5 of the Committee of Ministers to Member States on the processing of personal data in the employment context, point 10, 15 and 21).

On this point, it should also be noted that the 2015 legislator established that the fulfillment of the disclosure 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 purposes connected to the related relationship, including disciplinary findings, together with compliance with the data protection regulations personal data (see art. 4, paragraph 3, law 20.5.1970, n. 300, as replaced by art. 23, paragraph 1, Legislative Decree 14 September 2015, n. 151).

The company has therefore failed to adequately and in advance inform the complainants about the specific processing method actually carried out through the request to deliver the assigned devices and the subsequent imaging activity in view of the examination of the related contents, in violation of the provisions of the 'art. 13 of the Regulations and, as regards the complaint of 22 December 2018, the provisions of art. 13 of the Code (text in force at the time of making a copy of the devices of the relative complainant), which corresponds in the current legislation to the provisions of art. 13 of the Regulation. In the context of the employment relationship, the obligation to inform the employee is also an expression of the general principle of

fairness of processing (see Article 5, paragraph 1, letter a) of the Regulation and, as regards the complaint of 22 December 2018, v. art. 11, paragraph 1, lett. a) of the Code, text in force at the time of the duplication of the content of the devices of the relevant complainant, which corresponds, in the current legislation, to art. 5, par. 1, lett. a) of the Regulation).

3.2. With reference to the legal basis of the flow of data relating to complainants, which took place between Clear Channel Jolly Pubblicità S.p.A. and Clear Channel International LDT, separate legal entities both having their registered office in the European Union, the company declared (after initially providing the consent of one of the complainants to carry out - in general - audit activities; see section II , point 1.2., letter i), with reference to the complaint of 22 December 2018) that the parent company would have acted on the basis of its legitimate interest consisting in the need to defend and assert its rights, speculating the similar legitimate interest of company (see Article 6, paragraph 1, letter f) of the Regulation).

Based on what emerged during the investigation, the parent company played a role of impetus and constant coordination of the internal investigation concerning the activity of the complainants (and other employees of the Italian company), according to what was declared , following receipt of a report (prior to the adoption of an internal reporting system, which was approved in May 2019 - Protected Disclosure (Whistleblowing) Policy). Therefore, the company shared with the parent company personal data relating to the complainants as part of the internal investigation procedure coordinated by the parent company itself and initiated at the end of a process not yet formally regulated in accordance with the provisions of the law.

The legitimate interest of the owner (or third parties) is provided for by art. 6, par. 1, lett. f) of the Regulations, as a condition of lawfulness of processing by private parties, "provided that the interests or fundamental rights and freedoms of the data subject do not prevail", therefore upon the outcome of a comparative test carried out by the owner. Based on the provisions of the European data protection authorities (see Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46 / EC), the recurrence of this condition of lawfulness must be assessed by the owner following a careful assessment of the existence, in practice, of the requirements required by the legal system, based on a rigorous methodology, also and primarily with reference to the compliance of the treatment to be carried out with the principle of lawfulness.

In this regard, the requirements for the circulation of information relating to the ordinary performance of the employment relationship within groups of companies must be taken into consideration. Starting from the current legal framework (see art.1, l. 11 January 1979, n. 12; art. 1, paragraph 2, letter n), l. February 14, 2003, n. 30; art. 31, paragraph 1, legislative decree 10

September 2003, n. 276), the Guarantor specified that within the group of companies identified in accordance with the law (Article 2359 of the Italian Civil Code; Legislative Decree No. 74 of April 2, 2002), given that the companies of the group have a distinct and autonomous data controller in relation to the personal data of their employees and collaborators, "the subsidiaries and associates can delegate the parent company to carry out obligations in the field of work, social security and social assistance for the workers indicated by law [...] : this activity implies the designation of the parent company as data processor "(see Guidelines on the processing of personal data of workers for the purpose of managing the employment relationship employed by private employers, provision 23 November 2006, no. 53; para. 32).

Therefore, in the absence of any legal act (designation or similar) regulating the flows of personal data between the Italian company and the parent company, also in light of the aforementioned indices present in Italian legislation and what has already been clarified by the Guarantor, it is not allowed to resort legitimate interest as a suitable legal basis for the communication of employee data between the company and the parent company, given that this condition of lawfulness cannot be considered to exist only because other conditions, even more so if abstractly feasible, as in the present case, they do not recur. This also taking into account the nature and particular delicacy of the investigative activities carried out, capable of affecting a plurality of fundamental rights and freedoms of employees and third parties (on which later) which cannot fail to be the subject of a balancing test (see . Opinion 06/2014 cit.) Which also takes into account the opportunity to define the processing operations carried out by a person distinct from the owner. In any case, it does not appear that the company has carried out this comparative assessment, given that the documents only refer to the carrying out of an assessment on privacy, with the help of external consultants, in which, however, they do not appear to be the rights of the interested parties were taken into consideration (see note 19.6.2019, Annex 5) and, under different profiles, the alleged delimitation of the investigation commissioned to PwC in relation to which, as will be argued further on, was not provided suitable documentation.

Therefore, in relation to the profiles highlighted above, it appears that the company has processed the personal data of the complainants by sharing it with the parent company in the absence of one of the conditions indicated in art. 6 of the Regulation and therefore in violation of the provisions of art. 6 cit ..

3.3. With reference to the provisions, relating to the proposed control activities, by the documents "Security standards for the use of the IT equipment supplied and for the processing of company information" (dated February 2018), "Investigation Action Protocol" (dated November 2016), "Protect the data we use" (dated 25 May 2018) and "Policy on the acceptable use of

information security" (26.4.2018), adopted and considered fully operational by the company (on which see also previous paragraph 3.1 .), the following is observed.

Within the document "Safety standards for the use of the IT equipment supplied and for the processing of company information" it is envisaged that, with reference to "materials composed, sent or received via the company e-mail systems" […] The Clear Channel group reserves the right to check that the content of the emails is not illegal or contrary to its interests. [...] The use of passwords or folders with personal or common names does not make these messages private and the Company may override these passwords and / or access to these folders if it deems it necessary "; "The use of e-mail systems for occasional or fortuitous personal use is not encouraged even if it is tolerated from time to time. Personal emails will still be subject to the aforementioned policies and procedures "(p. 26). "All emails, both internal and external, remain the property of the Clear Channel group, which reserves the right to monitor their use for the purposes of system administration within the limits of the law and to verify any contents illegal or contrary to its activity. Any inappropriate or unlawful use of the system will be reported to the responsible executive. If a person is suspected of having violated this policy, the manager may ask the system administration to carry out an investigation "(p. 30). "The use of the internet for personal purposes is permitted during normal office hours only to solve an urgent problem. [...] The Clear Channel group has tools that allow you to monitor the use of the internet by the users of its information systems, in order to safeguard the security of their data and systems, in accordance with the laws in force. Any improper use of the system will be communicated to the manager responsible and may lead to disciplinary measures "(p. 32).

Furthermore, within the document "Protect the data we use", it is envisaged that, as part of the measures adopted "to protect the security of [...] personal data", the company may order "e-mail monitoring" (p. 9). Another part of the document also provides for the "monitoring of [the employee's] use of [...] information and communication systems to ensure compliance with [...] [the company's] policies" (p. 18). Within this document - although written in Italian - in the section relating to the exercise of rights regarding the protection of personal data, as regards the right to lodge a complaint with a supervisory authority, only the Information Commissioner's Office is mentioned. (data protection authority in the UK).

The document "Investigation Action Protocol", written in English, describes the internal investigation procedure following different types of events ("incidents"), within which the possibility of listening to the recordings of telephone calls, of monitoring o access the emails or electronic documents of employees and collaborators in pursuit of CCI's legitimate interest or to prevent

or combat crimes ("it may be necessary to listen to recorded telephone lines, monitor or access staff e-mails or electronic documents in pursuance of CCI legitimate business interests or to prevent or detect crime ") (p. 5).

Finally, in the document "Policy on the acceptable use of IT security" (26.4.2018), although with exclusive reference to the purpose of ensuring IT security and effective use of IT services, the company "reserves the right to inspect or monitor (directly or through the external service provider […]) any IT service of the company […] "; furthermore it is clarified that "except for the legal protections regarding personal data in the jurisdiction of residence, [...] employees must not have any further expectation of confidentiality when they are connected to the company network or use any company resource with a personal device or owned by the company ".

These documents, therefore, are intended to regulate the operating practices of the company in relation to the permitted use of company devices. Therefore, contrary to what the company believes (see previous point 2.1., Letter f), any infringement of the principles and provisions set forth in the matter of data protection of what is contained therein, far from being merely "virtual" , properly concerns the purposes and methods of the treatments that the company reserves the right to carry out in practice towards its employees and collaborators, although described in general terms without the necessary specifications (see in this regard the following paragraph 3.5., considering that specific treatments concerning the data referring to the complainants constitute in any case implementation of what is generally established by the company in relation to all workers), and this legitimizes the Authority's control activity on their compliance with the regulations in data protection (see provision point 29 October 2020, n.214, web doc. n. 9518890).

First of all, it emerges that the control activities envisaged by the aforementioned documents appear to be characterized by the systematic observation ("monitoring") of the e-mail flow, even of a private nature, with the possibility for the company to "override" the access passwords in the face of hypotheses represented in general and very broad terms (in case of opposition to one's own interests or activities or in the case of not better defined “illegal contents” or to “ensure compliance” with the company's “policies”). Likewise, it is possible to monitor the Internet browsing of employees in the face of completely generic occurrences ("in order to safeguard the security of their data and systems [and in the case of] any possible improper use of the system"), as well as accessing the contents of folders that have a suitable name (eg "personal or common names") to distinguish the content from that relating to the work activity. As part of the internal investigation procedure, it is also possible to access the content of any communication made by the employee (by telephone, email or documents drawn up) in the

presence of unspecified legitimate interests of the company or in the event that it is deemed necessary to pursue purposes. which, indeed, do not belong to the powers of private subjects ("prevent or detect crime").

The systematic and massive acquisition of personal data, even if not related to professional activity, as outlined in the aforementioned documents, does not comply with the principle of minimization (see Article 5, paragraph 1, letter c) of the Regulation) . Furthermore, the planned control activities do not envisage the adoption of preventive measures in the first instance (e.g. drafting of black lists of prohibited websites) or gradual checks, for example, on an aggregate basis, in order not to allow prolonged controls, constant or indiscriminate. This is in contrast with the principle of proportionality (see Article 5, paragraph 1, letter c) of the Regulation and art. 52 Charter of Fundamental Rights of the European Union).

Ultimately, the prefigured cancellation of any expectation of confidentiality does not comply with the aforementioned general principle if the employee is connected to the company network or uses a company resource even through personal devices (see on the point ECHR, Bărbulescu v. Romania [GC] , 5.9.2017 (rec. No. 61496/08), par. 80). In accordance with the constant orientation of the European Court of Human Rights, the protection of private life also extends to the workplace, considering that precisely when carrying out work and / or professional activities, relationships develop where the personality of the worker is expressed. (see articles 2 and 41, paragraph 2, of the Constitution). Also taking into account that the borderline between work / professional and strictly private sphere cannot always be clearly drawn, the Court considers that art. 8 of the European Convention on Human Rights set up to protect private life without distinguishing between the private sphere and the professional sphere (see Niemietz v. Allemagne, 16.12.1992 (rec. No. 13710/88), spec. Para. 29; Copland v. UK, 03.04.2007 (ref. No. 62617/00), spec. Par. 41; Bărbulescu v. Romania [GC], 5.9.2017 (ref. No. 61496/08), spec. Par. 70 -73; Antović and Mirković v. Montenegro, 28.11. 2017 (rec. No. 70838/13), spec. Para. 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).

Furthermore, with reference to the control activities that the company currently reserves to carry out within the terms provided for by the aforementioned documents "Safety standards for the use of the IT equipment supplied and for the processing of company information", "Investigation Action Protocol "," Protect the data we use "and" Policy on the acceptable use of IT

security ", it emerges that the company itself through access both to external data and to the contents of the mailbox during the employment relationship, and to " any recording of telephone calls made, both to the content of documents drawn up and / or in any case stored, can process personal data of employees in violation of art. 114 of the Code (where it refers to the observance of art.4, l. 20.5.1970, n. 300 as a condition of lawfulness of the processing; see, lastly, provision 11.3.2021, n. 90) information relating to the interested party not relevant for the purposes of assessing professional aptitude - also considering that even limited personal use of the devices themselves is allowed -, this in violation of art. 113 of the Code (where it refers as a condition of lawfulness of the processing the observance of art.8, l. 20.5.1970, n. 300 and art. 10 of legislative decree 10.9.2003, n. 276; a this last purpose Cass. civ., 19.9.2016, n. 18302 established that "acquiring and storing data that contain (or may contain) similar information already involves the integration of the prohibited conduct [...] even if the data are not subsequently It is not necessary to subject the collected data to any particular treatment to incur the offense, since the mere acquisition and conservation of their availability involves the violation of the legislative prescription "). This labor discipline, even as a result of the changes provided for by art. 23 of the legislative decree 14 September 2015, n. 151, does not allow the carrying out of activities suitable for carrying out massive, prolonged and indiscriminate control of the worker's activity and also constitutes one of the provisions of national law "more specific to ensure the protection of rights and freedoms with regard to the treatment of personal data of employees in the context of employment relationships "identified by art. 88 of the Regulation.

Finally, it is believed that the preparation of a plurality of documents containing references to the same control activity of the company, the absence of coordination between them on this point, the absence of the translation into Italian in relation to the Investigation Action Protocol and the Protected Disclosure (Whistleblowing) Policy and related information, the exclusive reference to the ICO as the supervisory authority at which to exercise the rights of the interested parties, the mere making available of documents in a shared folder, do not comply with the content of the obligation imposed on the data controller by art. 12 - in relation to art. 5, par. 1, lett. a) - of the Regulation according to which appropriate measures must be taken to provide the interested party with all the elements also relating to the exercise of rights "in a concise, transparent, intelligible and easily accessible form, with simple and clear language".

Therefore, the type and method of controls provided for in the aforementioned documents are, for the above reasons, in violation of the principles of minimization and proportionality (see Article 5, paragraph 1, letter c) of the Regulation and art. 52 Charter of Fundamental Rights of the European Union) as well as the provisions of art. 12, par. 1, of the Regulations in relation

to art. 5, par. 1, lett. a) (principle of transparency), and of arts. 113 and 114 of the Code in relation to art. 5, par. 1, lett. a) and 88 of the Regulation (principle of lawfulness).

In this regard, it is noted that the company, with a view to appreciable collaboration with the Supervisory Authority, during the procedure made itself available to modify the aforementioned documents and to bring their form and content into line with the provisions of the law. .

3.4. With exclusive reference to the complaint of 22 December 2018 and, in particular, to the request for access pursuant to art. 15 of the Regulations presented by the interested party to the company on 3 September 2018, it appears that the company itself has not provided any feedback, allegedly in compliance with the provisions of art. 2-undecies of the Code. This is in violation of the provisions of art. 12, par. 3 and 4 of the Regulations, as the data controller is required to provide the data subject, without undue delay, with the requested information; if the owner does not comply with the request, he must in any case inform without delay the interested party who has submitted a request to exercise the rights about the reasons for the non-compliance and the possibility of proposing a complaint to a supervisory authority and bringing a judicial appeal. The same article 2-undecies of the Code, in force since 19 September 2018 and which reproduced the case previously identified by art. 8, paragraph 2, lett. e) of the previous Code, provides that the owner can delay, limit or exclude the exercise of rights "with motivated communication and made without delay to the interested party".

Therefore, the company, from this point of view, has violated art. 12, par. 3 and 4 of the Regulations in relation to art. 15 of the Regulation.

3.5. Finally, it appears that the company, by copying all the contents (imaging) present on PCs and smartphones entrusted to the complainants, has collected, without distinction, all the data stored on the devices during the course of the work activity and also in the performance of activities. personal data (permitted by the company, albeit with limitations), thereby carrying out a check on the overall activity carried out by the interested parties over a large period of time (based on what was declared about two years and four months for the complaint of 22 December 2018 and about four years and eight months for the complaint of 23 November 2018).

Unlike what was held by the company in the defense briefs, the investigation activity carried out jointly with the parent company and at the instigation of the latter is not comparable to the investigative activity governed by the "Code of ethics and good conduct for the processing of personal data carried out for carry out defensive investigations ", in force at the time of the

facts (now see Annex A.2 to the Code, Deontological rules relating to the processing of personal data carried out to carry out defensive investigations or to assert or defend a right in court). First of all, it is noted that the documentation relating to the assignment entrusted to PwC, partially integrated after the notification of violations has been sent (see notes of 15.6.2020 and related attachments containing the list of "keywords"), does not present the characteristics of the investigator's appointment deed indicated by the aforementioned Code of Deontology (see Annex 4, note 8.11.2019 for the complaint of 22 December 2018 and Annexes 4 and 5 note 24.1.2020 for the complaint of 23 November 2018). In particular, there is no document that can be qualified as a "specific assignment" entrusted by the company to PwC, nor the specific indication of the right to be exercised in court, nor the main factual elements that justify the investigation and the reasonable term. within which this must be concluded (see art. 8, par. 3, Code of ethics quoted). It is also noted that while the activity of private investigators carried out on behalf of the employer, on the basis of a mandate and precise instructions, refers, as recognized by the constant jurisprudence of legitimacy, to situations in which the employee is objectively not engaged in carrying out the work activity, in particular during the period of illness or accident, or if he is in a place other than that where the service is to be performed (given that the activity of the investigative agency "cannot [] concern , in no case, neither the fulfillment, nor the non-fulfillment of the contractual obligation of the worker to perform his work, the non-fulfillment also being attributable, as the fulfillment, to the work activity, which is subtracted from the aforementioned supervision ", Civil Cassation, Labor Section, 4.9.2018, n. 21621), otherwise, in the specific case, the apprehension of all the contents present on the PC and smartphone service, c onfigures a processing operation consisting of the collection of information relating to the work carried out by the employee, including information relating to third parties (colleagues or strangers to the company structure), resulting in the inevitable impossibility of distinguishing ex ante (as the so-called theory on defensive controls, of pure jurisprudential creation, object of non-univocal applications, recalled by the company in its memoirs) any contractual offenses from non-contractual ones (taking into account, however, that, in most cases, the two hypotheses coincide).

The collection carried out also concerns a very wide type of data, contained respectively: in the communications made via e-mail and telephone (in the latter case, the data obtained from the company SIM), in the attachments sent and received, in the documents formed , in the chronology of the sites visited, this also in the performance of non-work activities (as permitted), with consequent processing of the private data of the worker and third parties. In this last regard, it should be noted that the same company recognized as possible the collection of data unrelated to the work activity or otherwise not relevant to the

subject of the investigation, declaring that it would have instructed PwC not to take them into account. In any case, given that during the investigation no documents relating to the assignment entrusted to PwC were produced from which it emerges that the company (as declared) has given the express indication to limit the investigation to the information extracted after using the previously identified "keywords" - which in any case are numerous and also contain terms that do not appear suitable for restricting the search to the work environment or, more generally, the subject of the survey - and not to take into account, and indeed eliminate as soon as possible, all non-relevant information that may have emerged from the outcome of the investigation, it is noted that the collection of personal data, entrusted in the specific case to a third party, constitutes a processing operation. Furthermore, it is recalled that, according to the constant jurisprudence of legitimacy "when the remote surveillance activity, activated by the employer for any purpose, also allows the mere" possibility of controlling the working activity "provided by the employee, the activity is not permitted unless following the successful completion of the guarantee procedures pursuant to art. 4, paragraph 2, [of the law of 20.5.1970, n. 300, previous text] "(Cass. Civ., 19.9.2016, n. 18302). The violation of the aforementioned provisions, which constitute a condition of lawfulness of the processing, therefore occurs also as a result of the sole preparation of activities suitable for carrying out the prohibited conduct.

The internal investigation activity carried out by the company for the declared purpose, legitimate in itself, of protecting its rights in the pre-litigation phase, in addition to the findings made above regarding the obligation to provide information and the communication of data to the parent company, does not actually assumed the characteristics of graduality, progressiveness and proportionality indicated several times by the ECHR jurisprudence (see ECHR, Bărbulescu v. Romania [GC], 5.9.2017 (rec. no. 61496/08), par. 121, which identifies the requisites considered relevant to the compliance assessment of the employer's correspondence and other communications control activities). In fact, upon receipt of an (unspecified) internal report, however managed in the absence of any formalization in a proceeding by the corporate group, a group of employees (including the complainants) were subjected to the most intrusive, i.e. the acquisition of a copy of all the operations carried out for a significant period of time during the work activity carried out by the employees themselves, in order to verify the validity of suspected illegal activities, the reliability of which has been subject to verification, at least towards the complainants (there is no information as to whether the suspicions were also considered justified towards the other employees subjected to the imaging of the devices), only after carrying out the checks.

There is no evidence in the documents, for example, that the company proceeded to find confirmation of its suspicions in the

first place through investigations on the documentary evidence present in the company archives, nor that it proceeded to a previous analysis of aggregate data (as instead from the same sustained: see previous point 1.2., letter h.). Nor, as argued above, is there evidence in the specific case that the investigation did not go beyond what was necessary to confirm the initial suspicion and that the control activity did not indiscriminately concern all the activity carried out by the complainants (with particular reference to the content of communications made). Ultimately, there is no evidence that at the time of carrying out the imaging activity it was not possible to carry out, at least in the first instance, other less intrusive measures.

Therefore, the internal investigation activity, carried out by the company in the terms described above, involved in the first place the processing of personal data of the complainants in violation of the principle of minimization and proportionality (see Article 5, paragraph 1, lett. c) and art. 52 Charter of Fundamental Rights of the European Union). Furthermore, the described treatments occurred in violation of the articles 113 and 114 of the Code, which refer to compliance with Articles 4 and 8 of the l. 20.5.1970, n. 300, as well as art. 10, legislative decree 2003 n. 276, as a specific condition of lawfulness of the processing (Article 5, paragraph 1, letter a) of the Regulation), as, as argued above, they made it possible to carry out a check on the activity of employees and to collect information on irrelevant facts for the purpose of assessing the professional aptitude of the employees themselves. This labor discipline constitutes one of the provisions of national law "more specific to ensure the protection of rights and freedoms with regard to the processing of personal data of employees in the context of employment relationships" identified by art. 88 of the Regulation (see, most recently, provision 11.3.2021, no. 90).

4. Conclusions: illegality of the treatment. Corrective measures pursuant to art. 58, par. 2, Regulations.

For the aforementioned reasons, the Authority believes that the declarations, documentation and reconstructions provided by the data controller during the investigation do not allow to overcome the findings notified by the Office with the act of initiation of the procedure and which are therefore unsuitable to allow the filing of this proceeding, since none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019. The processing of personal data carried out by the company in the terms described above is in fact illegal, in the terms set out above, in relation to articles 5, par. 1, lett. a) and c) (principles of lawfulness, correctness and minimization), 6 (legal basis of the processing), 12, par. 1, 12, par. 3 and 4 in relation to art. 15 (information, communications and transparent methods for exercising the rights of the data subject), 13 (information) and 88 (more specific provisions at national level) of the Regulation, in Articles 113 (data collection and relevance) and 114 (guarantees regarding remote control) of the Code and art. 11, paragraph 1, lett. a) and 13 of the Code, text in force at the time

of the facts subject of the complaint, (which correspond, in the current legislation, to articles 5, paragraph 1, letter a) and 13 of the Regulation) (principle of lawfulness and correctness and information).

Considering that the subject of the Guarantor's assessment specifically concerns the processing of personal data of the interested parties carried out by the company as part of the investigative activity carried out internally, the provisions of art. 160-bis of the Code, according to which "the validity, effectiveness and usability in judicial proceedings of deeds, documents and provisions based on the processing of personal data that do not comply with the provisions of the law or the Regulations remain governed by the relevant provisions procedural ".

Therefore, given the corrective powers attributed by art. 58, par. 2 of the Regulation, in light of the circumstances of the specific case:

- the company is enjoined to comply with the Regulations its processing with reference to the provisions of the internal regulations on the correct use of IT tools and related controls, within the terms set out in the motivation, also taking into account that the company itself has made available to adopt updated versions of the aforementioned documents (Article 58, paragraph 2, letter d), Regulations);

- the company is enjoined to comply with the Regulation the discipline of the communications of personal data, to the extent necessary, of its employees to the parent company (Article 58, paragraph 2, letter d), Regulation);

- the company is enjoined to provide feedback within the terms provided for by the law to the request for access whose non-response was complained of with the complaint of 22 December 2018 (Article 58, paragraph 2, letter d), Regulation);

- in addition to the corrective measure, there is a pecuniary administrative sanction pursuant to art. 83 of the Regulation, commensurate with the circumstances of the specific case (Article 58, paragraph 2, letter i), Regulation).

5. Injunction order.

Pursuant to art. 58, par. 2, lett. i) of the Regulations and art. 166, paragraphs 3 and 7 of the Code, the Guarantor provides for the application of the pecuniary administrative sanction provided for by art. 83, par. 5, lett. a) of the Regulations, through the adoption of an injunction order (Article 18, Law 11/24/1981, n. 689), in relation to the processing of personal data carried out by the company, whose unlawfulness was found, within above, in relation to articles 5, par. 1, lett. a) and c), 6, 12, par. 1, 12, par. 3 and 4 in relation to art. 15, 13 and 88 of the Regulation, in the articles. 113 and 114 of the Code and art. 11, paragraph 1, lett. a) and 13 of the Code, text in force at the time of the facts subject of the complaint, (which correspond, in the current

legislation, to articles 5, paragraph 1, letter a) and 13 of the Regulation), to the outcome of the procedure referred to in art. 166, paragraph 5 carried out in contradiction with the data controller (see previous points 1.4. And 1.5.).

Considering it necessary to apply paragraph 3 of art. 83 of the Regulation where it provides that "If, in relation to the same treatment or related treatments, a data controller [...] violates, with intent or negligence, various provisions of this regulation, the total amount of the pecuniary administrative sanction does not exceed the amount specified for the most serious violation ", considering that the ascertained violations of art. 5 of the Regulation are to be considered more serious, as they relate to the non-compliance with a plurality of general principles applicable to the processing of personal data, the total amount of the sanction is calculated in such a way as not to exceed the maximum permitted by law for the aforementioned violation. .

Consequently, the sanction provided for by art. 83, par. 5, lett. a), of the Regulation, which sets the maximum legal limit in the sum of 20 million euros or, for companies, in 4% of the annual worldwide turnover of the previous year, whichever is higher.

With reference to the elements listed in art. 83, par. 2 of the Regulations for the purposes of applying the pecuniary administrative sanction and its quantification, taking into account that the sanction must "in any case [be] effective, proportionate and dissuasive" (Article 83, par. 1 of the Regulations), it is stated that , in the present case, the following circumstances were considered:

a) in relation to the nature, gravity and duration of the violation, the nature of the violation which concerned the general principles of the processing was considered relevant; the violations also concerned the conditions of lawfulness of the processing (both the general ones and the more specific provisions regarding processing in the context of employment relationships), the provisions on information and the exercise of rights; in this regard, the provisions of art. 22, paragraph 13, d. lgs. n. 101 of 2018;

b) with reference to the willful or negligent nature of the violation and the degree of responsibility of the owner, the negligent conduct of the company and the degree of responsibility of the same that has not complied with the regulations on data protection relating to a plurality of provisions; in this regard it has been taken into account that the company has deemed it appropriate to consult external legal professionals before carrying out the processing;

c) the company cooperated with the Authority during the procedure and also declares its willingness to modify its internal regulations in accordance with the indications that will be provided by the Authority;

f) the absence of specific precedents (relating to the same type of treatment) charged to the company.

It is also believed that they assume relevance in the present case, taking into account the aforementioned principles of effectiveness, proportionality and dissuasiveness to which the Authority must comply in determining the amount of the sanction (Article 83, paragraph 1, of the Regulation), in firstly, the economic conditions of the offender, determined on the basis of the revenues achieved by the company with reference to the financial statements for the year 2019 (which recorded operating losses). Lastly, account is taken of the legal sanction imposed, in the previous regime, for the corresponding administrative offenses and the extent of the penalties imposed in similar cases.

In light of the elements indicated above and the assessments made, it is considered, in the present case, to apply against Clear Channel Italia S.p.A. (formerly Clear Channel Jolly Pubblicità S.p.A) the administrative sanction of the payment of a sum equal to Euro 75,000 (seventy-five thousand).

In this context, it is also considered, in consideration of the type of violations ascertained that concerned the conditions of lawfulness of the processing, the obligation to provide suitable information to the interested party and the exercise of the rights of the interested parties, who pursuant to 'art. 166, paragraph 7, of the Code and art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019, this provision should be published on the Guarantor's website.

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

Please note that, if the conditions are met, the penalty referred to in art. 83, par. 5, lett. e) of the Regulations.

WHEREAS, THE GUARANTOR

detects the unlawfulness of the processing carried out Clear Channel Italia S.p.A. in the person of the legal representative, with registered office in Viale Regina Margherita, 42, Rome (RM), C.F. 12710340154, pursuant to art. 143 of the Code, for the violation of art. 5, par. 1, lett. a) and c), 6, 12, par. 1, 12, par. 3 and 4 in relation to art. 15, 13 and 88 of the Regulations, in Articles. 113 and 114 of the Code and art. 11, paragraph 1, lett. a) and 13 of the Code, text in force at the time of the facts subject of the complaint, (which correspond, in the current legislation, to articles 5, paragraph 1, letter a) and 13 of the Regulation);

INJUNCES

pursuant to art. 58, par. 2, lett. d) of the Regulation to Clear Channel Italia S.p.A. to comply with the Regulations their processing with reference to the provisions of the internal regulations on the correct use of IT tools and related controls, within

the terms set out in the motivation, within 60 days of receipt of this provision;

INJUNCES

pursuant to art. 58, par. 2, lett. d) of the Regulation to Clear Channel Italia S.p.A. to comply with the Regulations the discipline of the communications of personal data, to the extent necessary, of its employees to the parent company, within 60 days of receipt of this provision;

INJUNCES

pursuant to art. 58, par. 2, lett. d) of the Regulation to Clear Channel Italia S.p.A. to provide feedback within the terms provided for by the law to the request for access whose non-response was complained of with the complaint of 22 December 2018, within 60 days of receipt of this provision;

ORDER

pursuant to art. 58, par. 2, lett. i) of the Regulation to Clear Channel Italia S.p.A. to pay the sum of 75,000 (seventy-five thousand) euros as a pecuniary administrative sanction for the violations indicated in this provision;

INJUNCES

also to the same Company to pay the aforementioned sum of 75,000 (seventy-five thousand) euros, according to the methods indicated in the annex, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the law n. 689/1981. Please note that the offender has the right to settle the dispute by paying - again according to the methods indicated in the annex - of an amount equal to half of the sanction imposed, within the term set out in art. 10, paragraph 3, of d. lgs. n. 150 of 1.9.2011 provided for the submission of the appeal as indicated below (Article 166, paragraph 8, of the Code);

HAS

the publication of this provision on the website of the Guarantor pursuant to art. 166, paragraph 7, of the Code and art. 16, paragraph 1, of the Guarantor Regulation n. 1/20129, and believes that the conditions set out in art. 17 of Regulation no. 1/2019.

Request Clear Channel Italia S.p.A. to communicate what initiatives have been taken in order to implement the provisions of this provision and to provide, in any case, adequately documented feedback pursuant to art. 157 of the Code, within 90 days from the date of notification of this provision; any non-response may result in the application of the administrative sanction

provided for by art. 83, par. 5, lett. e) of the Regulations.

Pursuant to art. 78 of the Regulations, as well as articles 152 of the Code and 10 of Legislative Decree n. 150/2011, an opposition to the ordinary judicial authority may be proposed against this provision, with an appeal filed with the ordinary court of the place identified in the same art. 10, within thirty days from the date of communication of the provision itself, or sixty days if the applicant resides abroad.

Rome, April 15, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Stanzione

THE SECRETARY GENERAL

Mattei