SEE ALSO NEWSLETTER OF 3 DECEMBER 2021

[doc. web n. 9722661]

Order injunction against TPER Trasporti Passeggeri Emilia Romagna S.p.A. - October 28, 2021

Record of measures

n. 384 of 28 October 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

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

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

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

GIVEN the documentation in the deeds;

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

RAPPORTEUR prof. Pasquale Stanzione;

WHEREAS

1. The complaint.

With a specific complaint, an employee of the Emilia Romagna Passenger Transport Company (hereinafter "TPER" or the "Company") represented profiles of possible violation of the personal data protection regulations as well as the sector regulations regarding remote workers' controls (art. 114 of the Code with reference to art. 300 of May 20, 1970, as amended by Article 23 of Legislative Decree No. 151 of September 14, 2015). In particular, alleged violations were alleged with regard to the processing of personal data of call center operators put in place by the Company through the telephone management system used for the user assistance service (inbound call center), through a dedicated platform. "Phones", created and supplied by IFM Infomaster S.p.A. (which also carried out maintenance activities on the platform), as data processor (Article 28 of the Regulation; see note XX and related annexes, in documents).

2. The preliminary activity.

In response to the specific requests of the Office, the Company, a company with full public participation, entrusted with the local public transport service of Bologna and Ferrara, and of other services (including parking control and issuing of badges in the territory of the Municipality of Bologna), which has about 2,500 employees, stated that (see note of the XX, in acts):

- "the company call center is one of the main channels for the dissemination of information to users (as explicitly required by art. 15 of the Service Contract [...]" and "the Directive of the President of the Council of Ministers January 27, 1994, provides that "the providers ensure full information to users about the methods of providing the services" and "prepare appropriate information tools, through the activation of telephone and telematic communication lines, which they periodically check for proper functioning (Article 3, letter. e)) ";

- “the Service Contract for the award of the automobile service in the Bologna basin provides, for example, in art. 14 paragraph 1 [that] "the concessionaire is required to equip itself with a monitoring and reporting system for the service provided [...] aimed at identifying preventive and corrective measures to be implemented to ensure the constant quantitative and qualitative adaptation of the service to needs of even potential users ";

- "the activation of telephone call recordings is therefore aimed at the timely fulfillment of the regulatory provisions and contractual obligations [... and to] settle any disputes (also to guarantee workers) and to allow the verification of the full correctness of the operations carried out";

- "to ensure the" recognition "and" traceability "of the operators [...] at the beginning of the phone call, the system communicates the operator's identification number to the user";

- “the telephone system used by the employees constitutes a work tool pursuant to article 4 of law 300/70, as amended by article 23 of legislative decree 14.9.2015 n. 151 [therefore ...] the recording of telephone calls between users and call center operators is allowed without the need to sign a prior trade union agreement or prior authorization from the INL [...] as adequate information is sufficient, which has been prepared and provided in paper format to the personnel concerned before activating the telephone registration system [in any case…] the trade unions […] have been informed in advance […]. The text of the information was also posted on the premises of the company call center ";

- “the data reporting activity is carried out in aggregate form (not nominative) to […] adapt the service offered to the needs of citizens (peak days and times); break down the calls by type of service (car services, railways, parking, car sharing); comply with the reporting obligations provided for in the service contract (generic data on the number of calls offered / answered and the timing of responses) ";

- the call center employee accesses "with his / her personal company credentials [...] the call center station [...] compost [a] from a PC with a commercial product from IFM Infomaster Spa installed which manages the telephone conversation and relating to [a] storage and archiving […] ”;

- "the recording of telephone conversations is started automatically, without any choice option either by the user or by the call center operator: at the end of the conversation, the recording is automatically saved in encrypted mode on a network folder which cannot be accessed without administrative privileges. It is not possible to listen to a telephone conversation again without using the specific application, which can be accessed using specific credentials provided only to the authorized persons specified in the company operating instructions IQC02 02 ";

- "the retention of recordings of telephone conversations is maintained, by company policy, for a period equal to 3 (three) months: at the end of this period the [a] record [e] is automatically deleted", this in order to " settle any complaints by users in relation to the use of certain services such as, for example, operations performed with the use of credit cards ";

- "the software platform that manages the telephone conversation [...] always contains and only grouped statistical data, which does not in any way allow to trace the operator who received the single call";

- "for each individual access, a registration must be promptly made in the call center file access register, which will report the information required by the company operating instruction IQC02 02";

- “the conversation listening procedure can be activated upon a reasoned request from the single operator […]; at the request

of the Citizen / user […]; by the company, in the case of complaints motivated in detail by citizens / users to verify the correspondence of what is reported; at the request of the public authority in the context of procedures of competence; randomly, on company initiative, to verify the quality standard of the service with the immediate cancellation of the data, if not critical ";

- "in case of access to the registration, the procedure foresees that this is moved to another directory and kept by the Managers indicated by the procedure until the end of the need for conservation";

- "once the requirements are over, until hypothetical causes are concluded, the registration will be canceled".

Subsequently, in order to complete the investigation framework with particular regard to the functioning of the system, the Office conducted an assessment activity, pursuant to art. 58 of the Regulation and 157 and 158 of the Code, towards the Company (see the minutes of the operations carried out in the 20th century, in documents), during which it was declared that:

- the Company "has always monitored the service first through statistical surveys, moving on to recording telephone calls in September 2018, with a view to guaranteeing a better quality of service [...]";

- "the Company has been using the inbound call center for many years, through a single number 051290290, to manage customer relations for the following services: public road transport in Bologna and Ferrara, regional railway services managed by TPER, management of markings ";

- "the call center employs about 20 employees, divided into 8 operator workstations, coordinated by a manager [of the service ...], moreover," in addition to the staff in stable mode to the function of call center operator, other employees are also temporarily assigned not suitable for the tasks for which they were hired (for example, drivers) ";

- "Out of the approximately 25,000 monthly telephone calls to 051290290, approximately 8,000 telephone calls are recorded per month, with peaks in some periods (for example in the month of October 2019 about 15,000 telephone calls were recorded" (see the IVR navigation tree annex 2 to the minutes);

- IFM S.p.A. of Genoa, “designated as Data Processor, created the call center platform called“ Phones ”[…] as a whole;

- the functionality of recording telephone calls and encrypting audio files (RecReviewer) is additional to the standard package and was acquired with a specific supplementary document "(see Annex 3 - minutes XX, copy of the contract with the IFM company);

- “users who are able to listen to phone calls, due to their corporate functions [… also include the], the call center manager”;

these subjects follow the specific company procedures established in this regard (see annex 4 - minutes XX, copy of the company procedure IQC02_02 rev. 1);

- "the technicians of the IFM company cannot access the registration data, stored on the TPER infrastructure, except for maintenance operations agreed between the parties";

- these accesses [...] take place exclusively via VPN which is opened only for carrying out the operations themselves and with limited and finalized access [... and] the operations carried out by IFM technicians on the data stored in the Phones platform are not tracked, while the he phone call replay application provides for the tracing of accesses and some operations including replay of phone calls "but" the encryption key of the recordings is known to IFM ".

During the on-site assessment, the functions relating to the re-listening of calls ("RecReviewer") were verified by accessing the "Phones" platform and, following the outcome of the investigations, it was ascertained that "in the database [were] stored the meta information of the recorded telephone calls, even after 90 days, and that such meta information includes the name of the operator, the date and time of the call and the calling telephone number. It was also found that the first available data date back to March 2018 "(see minutes XX, cit.).

With a note of the twentieth, in addition to the declarations made during the on-site assessment, also to dissolve the document production reserve advanced in the context of the inspection activity, the Company sent further documents and supplementary documents specifying, among other things, , that:

- the system "installed by the Supplier and tested in TPER on XX (as per IFM intervention report dated XX, doc. 4) [...] was activated only almost 7 months later, ie on XX, following the conclusion of the in-depth analysis [and requesting] a legal evaluation from a labor law expert on how to use the RecReviewer tool. In summary, TPER asked its consultant for confirmation of which were the prodromal activities to be implemented at the labor law level, and a verification of the text of the information intended for TPER workers [...] The lawyer verbally confirmed to the Company that the software recording of telephone calls in use by a call center could be considered a work tool [...] This analysis has been confirmed to date by the consultant involved "and by the" DPO [who carried out the] impact assessment pursuant to art . 35 of EU Regulation 679/2016 ";

- the data collected through the system "have never been used by TPER to monitor workers, so much so that no disciplinary sanctions or bonuses have been imposed / recognized on workers since the Company activated the recording of calls by call

center operators ";

- "the trade unions were convened at the time to inform them of the implementation of the new features in question and to share the text of the privacy information to be issued to the employees concerned by the processing" (see annex no. 2 and no. 3 note of the XX);

- following the preliminary investigation conducted by the Guarantor, TPER acted "with the Supplier to adapt the information systems so that in addition to the registrations, the meta-information is also deleted after 90 days, without prejudice to the right of further storage for the aforementioned purposes (protection of TPER in court in case of complaints, access to documents by citizens, fulfillment of legal obligations or requests from authorities [specifying that] the meta-information found during the inspection of the XX, [...] yes they refer to the tests and activities carried out by their IFM supplier on XX in order to verify the configuration of the call recording system "(see annex no. 4 note XX).

With a XXth note, the Office, on the basis of the elements acquired, notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in art. 58, par. 2, of the Regulation, inviting the aforementioned data controller to produce defensive writings or documents to the Guarantor or to ask to be heard by the Authority (Article 166, paragraphs 6 and 7, of the Code; as well as Article 18, paragraph 1, of the law no. 689 of 24 November 1981).

With the aforementioned note, the Office found that the Company has put in place, through the use of the system (so-called "Phones"), the processing of personal data of the complainant and other employees involved in the call center service, in a way that does not comply with the principles of "lawfulness, correctness and transparency", in violation of art. 5, par. 1, lett. a), and 13 of the Regulations, as well as in violation of articles 6 and 88, par. 2 of the Regulations and art. 114 of the Code, in relation to art. 4 of the l. May 20, 1970, n. 300; in a way that does not comply with the principles of "purpose limitation", "data minimization", "retention limitation", as well as "protection of personal data from design" and "by default", in violation of Articles 5, par. 1, lett. b), c) and e), and 25 of the Regulations; in the absence of adequate security measures to protect the integrity and confidentiality of the data, in violation of Articles 5, paragraph 1, lett. f) and 32 of the Regulations.

With a note dated the XXth, the Company sent its defense briefs, attaching the necessary documentation to prove the measures taken with regard to the treatments in progress against employees, and specifying, among other things, that:

- the service contract with the granting public body provides that "the contractor is required to equip himself with a system for

monitoring and reporting the quality of the service provided (Article 14), and the obligation to guarantee information to users on the service offered [...] by organizing a "call-center" service, referring to the complex of services entrusted, also using third-party structures, reachable by telephone [...] to provide information to users, to collect complaints, proposals and suggestions on the management of the service "(Article 15). [...]". There is also the obligation to "send a monthly report on the service provided, the minimum content of which must include [a] "final and updated statistics of the call-center parameters (calls received, calls accepted, calls accepted after queue, average waiting and conversation times)";

- "in order to be able to comply with the above, TPER has therefore deemed it necessary and necessary to activate the specific function of recording the calls received at the call center";

- "the need for registration was then felt also due to the new services offered to citizens, which include payments by credit cards" [and as] "an instrument aimed at the protection of workers in order to be able to adequately manage complaints or disputes by users who certainly may have as their object the work of the call-center staff ";

- "TPER [... has] acted with all the caution and in the legitimate conviction of using the instrument in question lawfully and of being able to consider the call center as a tool available to TPER personnel to perform their work";

- "in the event that this assessment had been subjected in any case to the conclusion of an agreement with the trade union, its failure to conclude would have compromised the provision of services to the community and determined the violation of the commitments undertaken towards the Public Body, or exposed the Company at the risk of incurring the penalties that the Service Contract provides even in the event of delay in fulfillment ";

- “the work of TPER [can] be criticized at the most in terms of involuntary and questionable erroneous interpretation of the rule referred to in art. 4 of the Workers' Statute, but never can he be charged with a preordained choice functional to obtaining the control and monitoring of his own workers ";

- the Company “has decided to convene the trade unions [… on] XX in order to comply with the indications” of the Guarantor, specifying that it has “initiated the necessary procedures required by law with its trade unions”;

- the "meta-information found in the application during the inspection of the XX, [... referred] to the tests and activities carried out by its supplier [...] the XX in order to verify the configuration of the calls [, and they] were present due to a system bug that TPER asked IFM to solve "[, being]" as of today, such information [...] kept for 90 days, as well as the telephone records "(see annexes nos. 3 and 4 screenshot of the query performed on the database and ticket to IFM for the management and resolution

of this bug);

- with regard to the information to the interested parties, the Company has undertaken to integrate it with regard to the profiles that were originally lacking or unclear, specifying however that "the workers were informed through the Disclosure to the Unions of the XX - prot. XX ";

- "on the retention time of the calls and related meta-data of the recordings, TPER, after appropriate internal assessments, has decided to set it at 90 days, considering this period of time adequate and not excessive in relation to the purposes it pursues [... given that] citizens could exercise the right of access to the documents in the event of administrative disputes for sanctions deriving from the violation of the highway code with respect, for example, to the ZTL access services also managed through the call-center: taking into account the notification time of the minutes of such sanctions […];

- in any case “the retention of data for the management of any complaints is absolutely possible and subject to the receipt of complaints or the occurrence of concrete and specific circumstances; circumstances that TPER will analyze and appropriately assess from time to time so that even its right of defense (towards the user and the Public Body to which it must report the work carried out) is not nullified by the cancellation of data and calls. On this point it is also specified that in the company policy ("Operating Instruction for the management of recordings of telephone calls to the Call CenteH '(see Doc. N. 7) it is expressly stated that" ... to operate a selective restore it will be necessary to written authorization from the Management ";

- with respect to the technical measures, the Company specified that “the password change after the first access cannot be performed for technical reasons of the product offered by IFM; on this point, IFM has reported to the Company that it is about to make these developments. In any case, TPER specifies that during the training provided to its staff it addresses the issue of password management and instructs the staff to change their passwords periodically [...] ";

- “the work of the IFM technicians is managed and" controlled "by virtue of the fact that it takes place via a VPN connection with a fixed IP and subject to prior agreement between the parties. Furthermore, it should be noted that IFM's work must follow the specific instructions of the Company and the agreements of the supply contract, given that IFM acts as a data processor. Among other things, TPER is not aware that it is subject to an obligation that imposes the tracking of such activities, obligations that it knows are expressly provided for in other cases (such as for example with respect to banking operations). Therefore, it is not considered that there is an express regulatory obligation that imposes such tracking on TPER ";

- in any case "the user creation and deletion activity logs are now active, as can be seen from the query on db" (see the

attached screenshots of this query, doc. n.10);

- “on the lack of a deletion log, it is specified that the calls are encrypted and that users without an" Administrator "profile on the IFM system cannot perform deletion operations; in the absence of a regulatory obligation that expressly requires the tracing of these operations, TPER has decided not to proceed with the implementation of this tracing, it being understood that this security measure will be taken into consideration in the assessments relating to the choice of the new system and call center provider ";

- in any case “the violation, if confirmed, must be considered limited to a very high number of interested parties; as mentioned, the call center operators were and are about twenty ";

- in the opinion of the Company "the staff [... is] aware of all the processing carried out through the call center, including that of recording calls [...]" and in any case the Company "does not believe that it has caused any harm to the interested parties" .

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

- “the Company has implemented some corrective actions by starting the process of industrial relations to reach an agreement pursuant to art. 4 l. 300/1970 to conform the treatments to the indications of the Guarantor. The Company took the opportunity to also regulate the treatments that it intends to implement using other technologies [...] that could fall within the scope of art. 4 l. 300/1970 ";

- "on the 20th the process relating to industrial relations was unsuccessfully concluded, the agreement was not signed, so authorization was requested from the territorially competent Labor Inspectorate, a procedure that has not yet been concluded" ;

- "at present, the call recording system covered by this investigation is not functioning and all the data and metadata collected and stored, including the telephone calls for which the replay was made, have been canceled and the processing has been interrupted" ;

- "on the 20th the Company updated the text [of the general information provided to all employees], sharing it with the staff, while the specific one relating to the processing of data of the personnel assigned to the call center will be updated following the outcome of the authorization procedure for to be able to take into account the indications of the Inspectorate […] [and] new

training courses will also be carried out in the light of the new functions that will be implemented taking into account the indications of the Guarantor and the Inspectorate ";

- "with regard to incoming calls to the call center, the brief information given to users has been corrected in which registration operations are no longer taken into account, as they are no longer carried out".

3. Outcome of the preliminary investigation.

On the basis of the regulations on the protection of personal data, the employer may process the personal data, also relating to particular categories of data (see Article 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 from the sector regulations (art. 6, par. 1, lett. c), 9, par. 2, lett. b) and 4; 88 of the Regulation). The processing is also lawful when it is "necessary for the performance of a task of public interest or connected to the exercise of public authority vested in the data controller" (art. 6, par. 1, lett. E), 2 and 3 of the Regulations; 2-ter of the Code, in the text prior to the changes made by Legislative Decree 8 October 2021, n. 139, in force at the time of the facts subject of the investigation).

The employer must also comply with national rules, which "include appropriate and specific measures to safeguard human dignity, legitimate interests and fundamental rights of the data subjects, in particular as regards the transparency of processing [...] and the systems of monitoring in the workplace "(articles 6, par. 2, and 88, par. 2, of the Regulations). On this point, the Code, confirming the system prior to the changes made by Legislative Decree 10 August 2018, n. 101, expressly refers to the national provisions of the sector that protect the dignity of people in the workplace, with particular reference to possible controls by the employer (articles 113 "Data collection and relevance" and 114 "Guarantees regarding remote control "). As a result of this postponement, and taking into account art. 88, par. 2, of the Regulations, the observance of articles 4 and 8 of the l. May 20, 1970, n. 300 and art. 10 of Legislative Decree no. 297/2003 (in cases where the conditions are met) constitutes a condition of lawfulness of the processing.

These rules constitute in the internal system those more specific and greater guarantee provisions referred to in art. 88 of the Regulation - for this purpose the subject of a specific notification by the Guarantor to the Commission, pursuant to art. 88, par. 3, of the Regulation - compliance with which constitutes a condition of lawfulness of the processing and the violation of which - similarly to the specific processing situations of Chapter IX of the Regulation - also determines the application of administrative pecuniary sanctions pursuant to art. 83, par. 5, lett. d), of the Regulations (see, with regard to the public work sector, most

recently, provision no. 273 of 22 July 2021, web doc. no. 9683814, spec. par. 4 and provision. 13 May 2021, no. 190, web doc. No. 9669974; see also the jurisprudence of the European Court of Human Rights, in the case of Antovic and Mirković v. Montenegro, application no. 70838/13 of 11.28.2017, which established that compliance of "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).

The data controller is, however, required to comply with the principles of data protection (Article 5 of the Regulation) and is responsible for the implementation of the technical and organizational measures appropriate to guarantee and be able to demonstrate that the processing is carried out in compliance with the Regulations (articles 5, par. 2, and 24 of the Regulations). The data must also be "processed in such a way as to guarantee adequate security" of the same, "including the protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage" (Article 5, paragraph 1, letter f); v. also art. 32 of the Regulation).

3.1. The data processing carried out through the "Phones" inbound phone call registration system.

From the assessment carried out, it appears that the Company had adopted, since the twentieth century, a system for the management of customer calls (inbound call center) which allowed the processing of personal data, referring to the staff assigned to the call center (or other personnel employed in this rotating service, who was unable to carry out ordinary duties, e.g. drivers temporarily unsuitable for the service).

At present, according to what was most recently declared by the Company, the system has been deactivated (see minutes of the hearing of the XXth).

In particular, the system for managing incoming customer calls (inbound call center), to which the telephone call recording function had been added at the request of the Company, was created, through the company IFM S.p.A. of Genoa, which also supplies the maintenance service. The system allowed part of the customer phone calls received by operators, also identified by their registration number, to be automatically registered on the platform called "Phones" and stored there for three months, after encrypting the audio files (additional "RecReviewer" functionality compared to the standard package offered by the Supplier).

In addition to the specific telephone call recording function, the possibility of replaying stored telephone calls was provided, through a specific procedure that could be activated by the Company or at the request of a citizen or an operator, as a rule, for

the management of any complaints, and " randomly, on company initiative, to verify the quality standard of the service with the immediate cancellation of the data, if not critical "(see minutes XX, cit.). The re-listening of the registration took place through a specific application, which was accessed by means of credentials provided only to authorized persons (see Company operating instructions IQC02 02). The procedure provided that the phone call to be listened to was moved to another directory and kept by the persons in charge indicated by the procedure until the end of the need for conservation (see minutes of the 20th, cit.).

The system also allowed the extraction of "data reporting in aggregate (non-nominative) form to [...] comply with the reporting obligations provided for in the service contract (generic data on the number of calls offered / answered and the timing of responses)" (see inspection report of the 20th, cit.).

As emerged during the checks carried out through direct access to the system during the inspections, the system also allowed the collection and storage of meta information relating to the recorded calls and, therefore, the processing of certain personal data relating to the employees assigned to the call. center (such as the name of the operator, the date and time of the call and the calling telephone number) with storage for a period of time that, at the time of the assessment, had not been defined by the Company (cf. p. 9, minutes of the 20th).

3.2. Lawfulness, correctness and transparency: the information to employees and the conditions of lawfulness of the processing.

The data controller must process the data "in a lawful, correct and transparent manner towards the interested party" (Article 5, paragraph 1, letter a) of the Regulation), adopting "appropriate measures to provide the interested party with all the information referred to in articles 13 and 14 […] "(article 12 of the Regulation).

The examination of the information provided to employees has highlighted that the Company has certainly informed the staff and, with a separate communication, also the trade unions of the definitive activation from the XXth of "a system for recording telephone calls between users and the employees, with the possibility of replaying a sample of the phone calls, also to settle any disputes "(see information in the documents); however, the information did not contain all the information required by art. 13 of the Regulations to ensure correct and transparent processing, such as, in particular, the indication of the rights of the data subjects referred to in Articles 15-22 of the Regulations and the right to lodge a complaint with the supervisory authority.

In addition, the document limited itself to mentioning the call recording function with respect to which it was specified that "the

data collected will be kept for the time strictly necessary to fulfill the purposes indicated, or 90 days unless disputes are to be kept until resolution" (cf. . information, in documents), without making any reference to the collection and storage of the so-called so-called meta information, referring to employees and their working activities, processing operations with respect to which, at the time of the verifications, the Company had not established a maximum retention period.

Again with reference to the transparency and correctness of the processing, it should be noted that the information expressly mentioned that "consent to the processing of data emerging from the recordings of telephone calls is not required, as it is aimed at fulfilling obligations deriving from a service contract of which Tper is an interested party ". If the text correctly excluded the use of consent as a prerequisite of lawfulness - given that the consent of the interested party cannot, as a rule, constitute a valid prerequisite of lawfulness for the processing of personal data when there is "an evident imbalance between the interested party and the owner "(see recital 43 of the Regulation), a circumstance that occurs in particular in the workplace (see, Data Protection Committee, Guidelines on consent pursuant to EU Regulation 2016 / 679- WP 259- of 4 May 2020, paragraph 3.1.1; see also Opinion 2/2017 on the processing of data in the workplace, adopted by the Article 29 Working Group adopted on 8 June 2017, WP 249) - the reference to the contract, as condition of lawfulness of the processing, is not relevant in the present case. The expression "necessary for the execution of a contract" referred to in art. 6, par. 1, lett. b) of the Regulation), refers to the case in which "the processing must be necessary to fulfill the contract with each interested party" and not instead as in the present case in the execution of a service contract between the owner and a third party, for example, with regard to the working context, "this assumption could allow, for example, the processing of information regarding salary and bank details to allow the payment of salaries" (see Opinion 6/2014 on the concept of legitimate interest of the data controller pursuant to Article 7 of Directive 95/46 / EC, adopted by the Article 29 Working Group on 9 April 2014, pages 19-20, WP 217). As also recently clarified by the Data Protection Committee, in fact, "it is necessary that there is a direct and objective link between the processing of data and the purpose of the execution of the contract with the data subjects" (see, Guidelines on consent pursuant to EU Regulation 2016/679, cit.).

The processing of employee data carried out by the Company through the system in question, being instead aimed at assisting users with a view to improving the quality and efficiency of the local public transport service for which the Company is the concession holder, can be rather considered in the context of the execution of a task in the public interest and of the obligations established by the sector regulations (Article 6, paragraph 1, letter e) of the Regulation). Given, then, the ownership

of the data processing of its employees and collaborators, for the management of the employment relationship, the processing must in any case also be carried out within the framework of the more specific national regulations that regulate the use of technological tools in the workplace and which, as clarified over time by the Guarantor (see par. 3 of this provision), constitute specific conditions of lawfulness of the processing (see, art. 5, 6 and 88 of the Regulation and 114 of the Code and art. 4, l. 300 of 20 May 1970). Furthermore, the Company itself refers to this sector regulatory framework in the text of the information originally provided to employees, which states that "Tper may use the information and data collected through the registrations for all purposes related to the employment relationship (for eg for bonus and disciplinary system) ", hypothesis expressly provided for by art. 4, paragraph 3, l. n. 300/1970.

For these reasons, the information document originally made available to employees did not contain all the elements expressly required by the Regulation, did not provide a clear and transparent representation of the overall processing carried out through the "Phones" system both with regard to some processing operations (eg . collection and storage of meta information) and with regard to the conditions of lawfulness of the same, in violation of Articles 5, par. 1, lett. a) and 13 of the Regulations.

However, it is acknowledged that during the procedure, the Company has updated the text of the general information provided to employees, intervening "further on the text of the information to make it more transparent and usable also with regard to the legal basis applied pursuant to art. 6 of the GDPR ", and reserving the right to prepare a specification relating to the processing of data of the staff assigned to the call center" upon the outcome of the authorization procedure to be able to take into account the indications of the Inspectorate "(see hearing report cit.).

3.3. The sector regulations regarding remote controls.

As emerged during the investigation, the system was aimed, on the basis of specific service contracts, to improve and make efficient the quality of the service provided in relations with users, therefore functional to respond to organizational and production needs, as well as efficiency and cost-effectiveness of the activity and of the public service provided.

As part of the investigations, it was verified that, in addition to allowing the reception and management of telephone calls and processing information necessary to respond to user requests, the system made possible other data processing operations relating to the staff employed at the call service. center. In fact, from the checks carried out on the specific characteristics of the system, it emerged that it was equipped with functions that also allowed the storage and listening of phone calls, as well as the collection of detailed information (meta information: the name of the operator, the calling number, the date and time of the

call - see p. 9 of the minutes of the 20th), directly associated with the employee who managed the phone call with the user.

In the specific context, as mentioned (see paragraphs 3 and 3.1 of this provision) the lawfulness of the processing is also connected to the observance of the sector regulations on the use of "tools from which the possibility of remote control of the 'workers' activity "(art. 5 and 6 par. 1, lett. c), and 88, par. 2, of the Regulation and 114 of the Code).

In these years the Guarantor, especially following the changes made to the l. May 20, 1970, n. 300, from art. 23 of d. lg. n. 151/2015, also addressed the issue of the distinction between paragraph 1 and paragraph 2 of art. 4 of the l. n. 300/1970 and the different legal regime that derives from it, evaluating, from time to time, the specificity of the treatments and systems used in practice by the employer, taking into account the guidelines of the jurisprudence, the Ministry of Labor and the National Inspectorate of labor, which apply this discipline as part of their institutional control functions (cf., among the numerous measures adopted most recently, provision no. 190 of May 13, 2021, web doc. no. 9669974; provision July 13 2016, n.303, par. 4.3, web doc 5408460 and provision 16 November 2017, n.479, web doc. .

With regard to the installation and use of support tools for the ordinary activity of call centers, the National Labor Inspectorate specified that "they can be considered work tools" (pursuant to Article 4, paragraph 2 of Law no. 300 / 1970) systems that "allow the mere connection between the call and the customer's personal data without further processing", vice versa, in other cases, for example when they also allow "further processing" to be carried out, they are in any case capable of creating a indirect and unintentional "monitoring of telephone activity" carried out by call center operators with the possibility of reconstructing their activity even indirectly (see INL, circular no. 4 of 26 July 2017, which contains operational indications on the installation and use of tools to support the ordinary operational activity of Call Centers).

Such tools that involve "an 'incidental' check on the worker's activity" therefore fall within the scope of art. 4, paragraph 1, of the l. n. 300/21970. del Lavoro ", see INL, circular no. 4 of 2017 cit.).

In line with this orientation, the Guarantor has already adopted, in the recent past, some specific decisions towards economic operators who used similar systems for managing relationships with customers and for improving the quality of the services offered, adhering to this interpretation. (see, provisions nos. 139 of 8 March 2018, web doc. 8163433 and 229 of the XX, spec. par. 2 and 3, web doc. 8987133).

As verified during the investigation, the system used by the Company was not limited to allowing the association between the incoming call and the customer's personal data to facilitate and simplify the activity of the call center operator in the rapid and

efficient management of user requests, nor did it consist of a mere computer archive for the sole use of employees who have relationships with users, but also allowed other processing operations and "further processing" and, specifically, the recording of calls and the storage of meta information relating to them directly associated with the names of the employees who had made them as part of their work.

In light of the foregoing considerations and the described characteristics of the system, which however did not allow to exclude the storage of information associated directly with employees ("the recording of telephone conversations is started automatically, without any choice option or by the user nor by the call center operator ", see note XX and inspection report, cit.), the pursuit by the Company of the specific purposes (" organizational and production ") through the aforementioned system should also have taken place in the compliance with the warranty conditions prescribed by article 4, paragraph 1 of law no. 300 of 1970 (trade union agreement or, alternatively, public authorization; see on the INL point, circular no.4619 of 24 May 2017).

Contrary to the original assessments of the data controller - carried out on the basis of opinions issued by its consultants -, the aforementioned system, in light of the regulatory framework for the sector and the aforementioned indications provided over time by the Guarantor, cannot, in fact, be considered among the "Tools used by the worker to make the performance work", pursuant to and for the purposes of art. 4, paragraph 2, l. n. 300/1970 rather, also due to the impossibility for the individual operator to deactivate the storage function, among the organizational tools referred to in art. 4, paragraph 1, l. 300/1970.

Therefore, if on the one hand the purposes that the Company intended to pursue with the management system of the telephone calls in question (ie that of guaranteeing the constant quantitative and qualitative adaptation of the service to the needs of users) are attributable to the legitimate "organizational and production needs […] ", Expressly without prejudice to the aforementioned article 4, paragraph 1, on the other hand, the Company has not activated, as it is required, the procedural guarantees prescribed by the same regulation (trade union agreement or authorization from the National Labor Inspectorate). Considering also that these guarantees cannot be satisfied by merely sending an information document to the trade unions, as was the case in the present case (see on this point, provision no. 282 of 17 December 2020, web doc no. 9525337, 303, par. 4.3, web doc 5408460 and 16 November 2017, n. 479, web doc. 7355533, par. 3.2.), the processing of personal data of employees, call center employees, carried out by the Company through the "Phones" system, appears to have occurred, up to the deactivation of the system and the interruption of the treatment (see, minutes of the hearing of the XX, cit.), in contrast with

the rules on the protection of personal data and with the relevant sector regulations, having the Company installed the same without activating the guarantee procedures provided for by the applicable sector law (in violation of articles 5, paragraph 1, letter a); 6, paragraph 1, lett. c); 88 of the Regulation and 114 of the Code, in relation to art. 4 of the l. May 20, 1970, n. 300).

3.4. Minimization, data protection by design and by default, and retention and purpose limitation.

According to the Regulation, the processing must concern only the data "adequate, relevant and limited to what is necessary with respect to the purposes for which they are processed" and the storage of data, in a form that allows the identification of the interested parties, is admitted "for a period of time not exceeding the achievement of the purposes for which they are processed" (art. 5, par. 1, lett. c) and e) of the Regulation). Also in consideration of the risk incumbent on the rights and freedoms of the data subjects, the data controller, based on the principles of data protection by design and by default (Article 25 of the Regulation; see also Recital no. 75 and 78), must implement "adequate technical and organizational measures [...] aimed at effectively implementing the principles of data protection, such as minimization, and integrating the necessary guarantees into the processing in order to meet the requirements of [...] regulation and protect the rights of interested parties "(par. 1).

As can be seen from the overall investigation activity, the system allowed, instead, the systematic storage and conservation of meta information relating to the calls recorded for a time, at the date of the investigations, not yet defined by the owner (see p. 9 minutes of the 20th from which appears, in fact, that the data on the system dated back to 2018).

The data controller, in addition to respecting the principle of "data protection by design" (Article 25, paragraph 1, of the Regulation) - by adopting appropriate technical and organizational measures to implement the principles of data protection (Article 5 of the Regulation) and integrating in the processing the necessary guarantees to meet the requirements of the Regulation and protect the rights and freedoms of the data subjects - must also, in accordance with the principle of "data protection by default" (Article 25, par. 2 , of the Regulation), make choices that ensure that only the processing strictly necessary to achieve a specific and lawful purpose is carried out by default. This means that, by default, the data controller must not collect personal data that are not necessary for the specific purpose of the processing (see "Guidelines 4/2019 on article 25 Data protection by design and by default ", Adopted on 20 October 2020 by the European Data Protection Board, spec. Points 42, 44 and 49).

As recently highlighted by the Guarantor (see, with regard to specific processing in the workplace, provision n.235 of 10 June

2021, web doc. N.9685922; but see with regard to the processing of user and employee data through a service booking system at the counter, provision 17 December 2020, n.282, web doc. n.9525337), the data controller, even when using products or services made by third parties, must check of the Data Protection Officer where appointed, 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 giving the necessary instructions to the service provider (see articles 5, par. 2, 24, 25 and 32 of the Regulation). In this perspective, the data controller must ensure that, in particular, the functions that are not compatible with the purposes of the processing are deactivated, or are in contrast with specific sector regulations provided for by the law and, in particular, with regard to in this case, the national and greater protection regulations for the interested parties with regard to processing in the workplace (Article 88 of the Regulation in relation to Articles 113 and 114 of the Code).

For these reasons, taking into account the organizational and efficiency needs of the service pursued with the aforementioned system, the applicable sectoral regulatory framework (Article 4, paragraph 1, Law no. ., provision 16 November 2017, n. 479 web doc. 7355533, cit. and provisions 22 December 2016, n. 547, web doc. n. 5958296, par. 3.5 and 13 July 2016, n. . 5, cit .; but see also Guidelines for e-mail and internet, provision of 1 March 2007, no. 13, web doc. No. 1387522, spec. Par. 4, with principles that can be considered all now valid; more generally, Council of Europe, Recommendation of 1 April 2015, CM / Rec (2015) 5, spec.princ. 14-15 and Article 29 Working Party, Opinion 2/2017 on data processing at work, WP 249, paragraph 5), the specific processing operations consisting in the collection and storage for an indefinite period of time of the meta information referring directly to employees and their att work, do not comply with the principles of minimization and limitation of data retention as well as protection of personal data from the design stage and by default, in violation of Articles 5, par. 1, lett. c) and e), and 25 of the Regulations.

The described treatments cannot be considered justified even for further purposes, related to the use in the context of any complaints by citizens and users, also invoked by the Company and referred to in the information to employees. The processing of personal data carried out for the purpose of protecting rights must in fact refer to ongoing disputes or pre-litigation situations and not to abstract and indeterminate hypotheses of possible defense or protection of rights, given that this extensive interpretation would be elusive of the provisions on legitimation criteria. of the processing (this general principle was, lastly, reaffirmed by the Guarantor precisely with regard to the working context in the "Provision containing the provisions

relating to the processing of particular categories of data, pursuant to art. 21, paragraph 1 of the legislative decree . 10 August 2018, no. 101 ", Annex 1, par. 1.3, letter d), doc. web n. 9124510).

Given, then, the principle according to which the data must be "collected for specific, explicit legitimate purposes, and subsequently processed in a way that is not incompatible with these purposes" (Article 5, paragraph 1, letter b) of Regulation) it is finally pointed out that, although the Company has declared that the data collected by the system have "never been used by TPER to monitor workers, so much so that no disciplinary sanctions or bonuses have been issued / recognized to workers since the Company activated the recording of calls from call center operators ", during the investigation it emerged that the same had in any case reserved, in general, the possibility of using the data collected through the system for all purposes connected with the management of the employment relationship (art. 4, paragraph 3, of law no. 300/1970), as shown in the text of the information in the documents.

In this regard, although there is no evidence in acts of processing carried out by the Company for these purposes (reason for which it is believed to file the dispute in relation to this profile), it seems necessary to clarify that the current regulatory framework allows the data collected pursuant to art. 4, paragraphs 1 and 2 of law no. 300/1970 can be used by the employer "for all purposes related to the employment relationship" on condition that "the worker is given adequate information on how to use the tools and carry out controls and in compliance with the provisions of Legislative Decree No. 196 of 30 June 2003 "(Article 4, paragraph 3 of Law No. 300/1970).

As recently highlighted by the Guarantor with the provision of 13 May 2021, n. 190, "the current regulatory framework allows the owner (employer) to use the identification data of the workers, for further purposes, as part of the management of the relationship, only the information collected in compliance with the conditions and limits provided for by art . 4 "of the l. n. 300/1970 (in this case with reference to paragraph 1) and therefore "within the limits in which the original collection was lawfully carried out". This framework therefore presupposes an autonomous determination by the owner regarding the use of the information, where already lawfully collected in compliance with the conditions and limits provided for by art. 4, paragraphs 1 or 2 of the l. n. 300/70, also for further processing necessary for the management of the employment relationship (Article 4, paragraph 3 of Law 300/1970). Such subsequent and any processing operations presuppose compliance with the reference regulatory framework both in terms of remote workers' checks (pursuant to paragraphs 1 and 2) and in terms of data protection. So much so, not only with regard to the need to provide the interested parties with all necessary information to

ensure employees full awareness of the further treatments that the employer reserves the right to carry out (a circumstance that does not occur in the present case), but also through the appropriate configuration of the system so that only the necessary data are collected, within the time limits identified in relation to the main purpose for which the system was adopted (on this point, see Provv. May 13, 2021, n. 190, doc web n. 9669974, par. 3.3 .; see already provision 24 May 2017, n. 247, web doc. 6495708, spec. point 5.3 and letter e) device).

3.5 The security of the processing.

According to the Regulation, the data must be "processed in such a way as to guarantee adequate security of personal data, including protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage. "(Article 5, par. 1, letter f), of the Regulations).

In this regard, art. 32 of the Regulation establishes that "taking into account the state of the art and the costs of implementation, as well as the nature, the object of the context and the purposes of the processing, as well as the risk of varying probability and severity for the rights and freedoms of natural persons, the data controller and the data processor implement adequate technical and organizational measures to ensure a level of security appropriate to the risk "and that" in assessing the adequate level of security, special risks are taken into account presented by the treatment that derive in particular [...] from the unauthorized disclosure [... of] personal data transmitted, stored or otherwise processed ".

In relation to the "Phones" recording system for inbound telephone calls, created by the company IFM Infomaster S.p.A, certified on company systems, it is noted that some of the technical measures adopted do not appear adequate to protect the personal data contained therein. First of all, it was ascertained that the password set by the administrator, when creating a new user, did not necessarily have to be changed at the time of the user's first access (see p. 7 of the report of the XX). In this way, the confidential nature of the credentials for accessing personal data is potentially lost by authorized parties, not only towards the system administrator but also towards other users. Moreover, the risks would be amplified where the username and password chosen by the administrator are set according to a standard format, known at company level and therefore easily replicable by other users (e.g. username equal to first name, last name and first password equal to last name).

With regard to the tracing of accesses to recorded telephone calls, the recordings - log file - of the operations carried out do not appear to be sufficient, since the recording of the work of the IFM company technicians on the system or of the operations of creation and cancellation of the users has not been foreseen. cancellation of a registration (see p. 9 of the minutes of the

XXth). Such missing registrations therefore do not allow the data controller to have knowledge, with certainty and in an exhaustive manner, of all the accesses to the recorded telephone calls, nor do they make him able to document such accesses.

This obligation for the owner, already present in the previous regulatory framework (pursuant to the technical specification referred to in Annex B to the Code, in the text prior to the amendments referred to in Legislative Decree no. as claimed by the Company in the defense briefs, from the obligation to adopt technical and organizational measures aimed at guaranteeing an adequate level of security also with respect to the risk of unauthorized disclosure or unlawful access to data (Article 32 of the Regulation) and the related obligation to prove its adequacy (articles 5, par. 2, and 24 of the Regulations). By reason of the "general responsibility" of the data controller (Article 5, paragraph 2 of the Regulation), the same is, in fact, required to "implement adequate and effective measures [and ...] demonstrate the compliance of the processing activities with the […] Regulation, including the effectiveness of the measures "(see recital 74 as well as articles 24 and 25 of the Regulation), providing the necessary information to the service provider for this purpose (article 28 of the Regulation).

For these reasons, the Company was responsible for the failure to adopt adequate technical and organizational measures to ensure the confidentiality and integrity of personal data processed through the "Phones system, in violation of Articles 5, paragraph 1, lett. f) as well as 32 of the Regulation.

4. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the data controller in the defensive writings □ the truthfulness of which one may be called to answer pursuant to art. 168 of the Code □ although worthy of consideration and indicative of the full collaboration of the data controller in order to mitigate the risks of the processing, compared to the situation present at the time of the investigation, they do not however allow to overcome the findings notified by the Office with the act of initiation of the procedure and are therefore insufficient to allow the filing of this proceeding, since none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

From the checks carried out on the basis of the elements acquired, also through the documentation sent by the data controller, as well as from the subsequent evaluations, the non-compliance of certain treatments concerning personal data of employees was ascertained, through the "Phones" system activated, in definitive way, from the XX.

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

689/1981, according to which the laws that provide for administrative sanctions are applied only in the cases and times considered in them. This determines the obligation to take into account the provisions in force at the time of the committed violation, which in the case in question - given the permanent nature of the alleged offenses - must be identified in the act of cessation of the unlawful conduct. In acknowledging that the data controller has, in the course of the investigation, taken steps to conform the treatment to the principles of the Regulation, to adopt appropriate technical and organizational measures to guarantee a level of security adequate to the risk presented by the treatment, it is considered that, given the cessation of illicit treatments which occurred later in May 2021, the Regulations and the Code constitute the legislation in the light of which to evaluate the treatments in question.

The preliminary assessments of the Office are therefore confirmed and the unlawfulness of the processing of personal data carried out by the Company is noted as, until the deactivation of the system (XX) occurred in a manner that does not comply with the general principles of treatment and in violation of Articles 5, par. 1, lett. a), b), c) and e), 6, 13, 25, 32 and 88, par. 2 of the Regulations and art. 114 of the Code.

The violation of the aforementioned provisions also makes the administrative sanction applicable pursuant to art. 58, par. 2, lett. i), and 83, para. 4 and 5, of the Regulation.

In this context, considering that the conduct has exhausted its effects (see the minutes of the hearing of the XXth, which states that "at present the call recording system subject of this investigation is not functioning and all data and metadata collected and stored , including the phone calls for which the replay was made, have been canceled and the processing has been interrupted "), the conditions for the adoption of corrective measures, pursuant to art. 58, par. 2, of the Regulation.

5. Adoption of the injunction order for the application of the pecuniary administrative sanction and ancillary sanctions (Articles 58, paragraph 2, letter i), and 83 of the Regulations; art. 166, paragraph 7, of the Code).

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

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

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

For the purpose of applying the sanction, it was considered that, although the Company declared that the employees assigned to the call center were about 20, the circumstance under which "in addition to the staff in stable mode for the function of call center operator, also assigned other employees temporarily unsuitable for the tasks for which they were hired (for example, drivers) "does not allow the total number of employees involved in the treatment to be determined with certainty, as it must therefore be assumed that, albeit occasionally, the violations have interested a greater number of interested parties. The following were also considered: both the specific nature of the processing - initiated in a manner that does not comply with the sector regulations on the use of technological tools in the workplace and the indications provided over time by the Guarantor, for the profiles of competence - and the prolonged duration of the treatment - which lasted from the XX to the XX, the term of the definitive cessation of the same.

On the other hand, it was considered that the data controller in any case collaborated during the investigation, taking steps to adopt, already following the inspection activity conducted by the Office, some first corrections to the treatments subject to the complaint and to initiate at the same time, the necessary investigations to ensure full compliance of the processing with the provisions on the protection of employee data, in compliance with the principle of accountability. For the purposes of measuring the overall sanction, it was also considered that the data controller, whose technical and organizational choices were made on the basis of the evaluations expressed, even informally, by their consultants and by the Data Protection Officer, had trusted in the lawfulness of the treatments put in place.

Furthermore, there are no previous violations committed by the data controller or previous provisions pursuant to art. 58 of the Regulation.

Due to the aforementioned elements, assessed as a whole, it is considered to determine the amount of the financial penalty, in the amount of € 30,000.00 (thirty thousand) for the violation of Articles 5, 6, 13, 25, 32 and 88 of the Regulation, as well as 114 of the Code.

Taking into account the specific risks for the rights of data subjects deriving from the use of systems that also involve remote

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

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

WHEREAS, THE GUARANTOR

detects the unlawfulness of the processing carried out by TPER Trasporti Passeggeri Emilia Romagna S.p.A. for the violation of articles 5, 6, 13, 25, 32 and 88 of the Regulation and 114 of the Code, in the terms set out in the motivation;

ORDER

to TPER Passenger Transport Emilia Romagna S.p.A. in the person of the pro-tempore legal representative, with registered office in Bologna, Via Saliceto n. 3, P.I. 03182161202, pursuant to art. 58, par. 2, lett. i), and 83, par. 5, of the Regulations, to pay the sum of € 30,000.00 (thirty thousand) as a pecuniary administrative sanction for the violations indicated in the motivation; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within thirty days, an amount equal to half of the sanction imposed;

INJUNCES

to TPER Passenger Transport Emilia Romagna S.p.A. to pay the sum of € 30,000.00 (thirty thousand) in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, according to the methods indicated in the annex, within thirty days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the l. n. 689/1981;

HAS

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

the annotation of this provision in the internal register of the Authority, provided for by art. 57, par. 1, lett. u), of the Regulations, violations and measures adopted in compliance with art. 58, par. 2, of the Regulation.

Pursuant to art. 78 of the Regulation, of art. 152 of the Code and 10 of Legislative Decree 1 September 2011, n. 150, against this provision, it is possible to appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the applicant resides abroad.

Rome, October 28, 2021

PRESIDENT

Straction

THE RAPPORTEUR

Stanzione

THE SECRETARY GENERAL

Mattei