SEE ALSO Newsletter of 10 September 2021

[doc. web n. 9698724]

Injunction order against Roma Capitale - 22 July 2021

Record of measures

n. 294 of 22 July 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 / EC, "General Data Protection Regulation" (hereinafter the "Regulation");

GIVEN the legislative decree 30 June 2003, n. 196, "Code regarding the protection of personal data", as amended by Legislative Decree 10 August 2018, n. 101, containing provisions for the adaptation of national law to the Regulation (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 April 2019, published in the Official Gazette n. 106 of 8 May 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 of the Office made by the Secretary General pursuant to art. 15 of the Guarantor Regulation n. 1/2000 on the organization and operation of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web n. 1098801;

SPEAKER Attorney Guido Scorza;

1. Introduction

From a report submitted to the Authority in the month of XX it emerged that, for the issue of the badges certifying the payment of parking in the parking lots of Roma Capitale, it is required to insert, in the appropriate parking meters, the license plate of

the vehicle for which make the payment.

2. The preliminary activity

In relation to the case, an investigation was launched, during which an inspection was also carried out in collaboration with the special Privacy Unit of the Guardia di Finanza.

From the assessment it emerged that, with the resolution of the Capitoline Council no. XX of the XX (annex 3 of the XX minutes), have been entrusted (notes no. XX of the XX and no. XX of the XX) to Atac s.p.a. services complementary to scheduled public transport, relating to the management of exchange parking lots and parking with tariffs on the road, under the responsibility of Roma Capitale, for the period XX (extended until the XXth by virtue of the Deliberation of the Capitoline Assembly no.).

On the proposal of Atac s.p.a. (note of the twentieth, attached to the aforementioned resolution), some parking meters under management have been subject to technological adaptation, in order to allow payment also by debit / credit cards, the personalization of payment by inserting the vehicle number plate (with the consequent no need for the user to display the payment coupon) and the possible activation of additional services on the parking meter (eg payment of sanctions / taxes, purchase / renewal of public transport tickets). This phase of "modernization" was concluded in the month of XX, starting from which the new parking meters became operational (note no. XX of the XX of Atac s.p.a., annex 4 of the XX minutes).

As regards the functional architecture of the system, Atac s.p.a has created a centralized system that collects the information (time, date of start and end of parking, the amount paid and the license plate) relating to the payment of the parking. carried out via apps made available by various operators (myCicero, easyPark, etc.) or "evolved" Pay & Go parking meters (managed by the company Parkeon s.r.l., now Flowbird Italia s.r.l.) and to make them available both to traffic auxiliaries for the purposes of checking " payment of the parking has been made (through the use of the E-Multe-S app, installed on company smartphones), and to the internal staff of the company for administrative management purposes.

During the inspection, the involvement of Atac s.p.a. was ascertained. and Flowbird Italia s.r.l. in the treatment in question but, in both cases, the relative relationship was not regulated pursuant to art. 28 of the Regulations before the start of the treatment.

On this point, in fact, although Roma Capitale has confirmed that it has foreseen that Atac s.p.a. operated as data processor, during the investigation it emerged that "it does not appear that such an appointment has been made". Furthermore, with

regard to the role assumed by third parties (Flowbird Italia s.r.l), Roma Capitale stated that "having no relationship with said parties [...] it has not formulated any appointment as responsible for said parties" (minutes XX).

With regard to the obligation to provide information to interested parties regarding the processing described above, Roma Capitale stated that "at the moment the parking meters themselves do not contain any text or any reference to the same, I do, however, provide printouts of the ways in which the The display of the parking meters will provide a link to the websites of the Municipality of Rome and Atac spa on which the specific information will be available, this procedure is being evaluated "(annex 5 of minutes XX).

As regards the number of interested parties involved, the treatment in question regards, broadly speaking, all those who use the parking service in the territory of the Municipality of Roma Capitale (residents and non-residents). During the checks carried out (table dbo.sostainizio, minutes of the XX, annex 9) it emerged that, up to the XX, 8,600,000 data relating to the stops made by the vehicles have already been recorded in the system.

Regarding the definition of the retention times of the data collected through the aforementioned parking meters, as well as the adoption of appropriate technical and organizational security measures, Roma Capitale stated that it does not process "in any way the personal data of users who use the payment service parking through the parking meters; therefore, with specific regard to [...] the security measures and the retention times of the data in question, [...] the competence lies with Atac s.p.a. " (minutes XX).

During the checks carried out at the headquarters of Atac s.p.a., the company stated that (minutes of the XXth) “at the moment no data has been deleted; however, the definition of their conservation times is currently being studied and decided ". In fact, it was found that, at the time of the verifications (minutes XX), no measures had been implemented for the deletion of data or technical measures suitable for the conservation of personal data, in anonymous or pseudonymous form, had been adopted.

In particular, by accessing the company system, it was possible to verify that (report XX):

- in the dbo.Multe table, in which the information relating to fines raised by traffic auxiliaries is stored, the information relating to the license plate is stored in clear text for about 60 days (ie from the XX, date of access to the system); before that date, the "targa" field is not completed;

- in the dbo.sostaInizio table, the data relating to the period of validity of a payment (date, time of start and end of parking, vehicle plate, etc.) starting from the XXth are stored; of the aforementioned data, only those relating to the last 60 days present

the information relating to the license plate stored in clear text; for the previous period, the "plate" field is not completed, while the computer fingerprint obtained by applying the MD5 algorithm on the value of the "plate" is kept, before its cancellation;

- by means of the “Movements detail” function, it is however possible to view all the number plates relating to the payments of the stops starting from XX, stored in clear text.

Finally, with regard to the technical and organizational measures adopted, it was ascertained (minutes XX) that:

- some data flows “to and from” the ATAC system do not make use of secure communication channels. In particular, to check that the parking has been paid, the traffic auxiliaries access the ATAC system with the "E-Multe-S" app which communicates with the server in question using the http protocol (minutes of the 20th), by transmitting the data in clear text;

- the authentication system does not guarantee suitable security measures regarding the format of the passwords and their storage in the database. The passwords used for the authentication of the auxiliaries are in fact stored in clear text within the database (minutes of the XXth) and made up of 5 characters, as confirmed during a simulation of use of the app in question (minutes of the XXth).

- furthermore, no mechanism has been implemented that allows the traceability of the operations carried out (application log) by system users on personal data, whether they are system administrators or back office operators and traffic auxiliaries (minutes of the XXth). This deficiency excludes the possibility of carrying out ex post checks on the work of employees with respect to the computerized processing of a large volume of data relating to a large number of interested parties, data that can potentially lend themselves to fraudulent uses to their detriment, allowing to detect the status absence from home or presence in a certain area of the city in a given period of time.

With a note of the XX (prot. No. XX), the Office, on the basis of the elements acquired, notified Roma Capitale, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in art. 58, par. 2, of the Regulations, inviting the aforementioned owner to produce defensive writings or documents to the Guarantor or to ask to be heard by the Authority (Article 166, paragraphs 6 and 7, of the Code; as well as Article 18, paragraph 1, of Law no. . 689 of 11/24/1981). With the aforementioned note, the Office found that Roma Capitale has carried out processing of personal data collected through the new parking meters installed in the area, without having provided suitable information to the interested parties, in the absence of definition of the role of the external subjects involved in the processing, without having defined the retention times of the collected data and without having adopted suitable security measures, in violation of articles 5, 12, 13,

25, 28 and 32 of the Regulation.

With the notes prot. n. XX del XX and XX Roma Capitale sent its defense writings in relation to the notified violations to the Guarantor, attaching, among other things, a technical report prepared by Atac s.p.a .. In particular, from this last report it emerged that:

- “on the 20th date the Mobility and Transport Department of Roma Capitale appointed Atac s.p.a. Responsible for the processing of personal data acquired in execution of the Service Contract signed on XX with Roma Capitale and approved with Resolution XX ";

- Roma Capitale authorized, with note no. XX del XX, Atac s.p.a to name "Flowbird s.p.a." (sub) data processor, whose appointment was formalized on XX;

- on XX Roma Capitale and Atac s.p.a. have published the information on the processing of personal data in question on their respective institutional sites. Furthermore, by intervening on the parking meters, "a summary information was added to the home screen of the advanced parking meter, together with the indication of the link of the ATAC website containing the complete information" (see note of XX, annex 10-bis and annex 17) ".

Regarding the storage times and the technical and organizational measures adopted, from the aforementioned technical report it emerged that, starting from the month of XX, Atac s.p.a. has implemented the following measures:

- “identification of users through the use of personal passwords with a minimum length of 8 characters subject to encryption;

- system log at the level of access to the database through the registration of both successful accesses and unsuccessful attempts; various logs of an application nature that allow, for example, the tracking of the operator (Traffic Auxiliaries) who carried out a specific fine and the tracking of the operator (Traffic Auxiliaries) to which the system responded following a license plate query ;

- one-way encryption of license plates older than 60 days with MD5 hash algorithm;

- application of the digital certificate on the back office system for the management of the assessment notices; application of the digital certificate on the communication channel between the auxiliary's smartphone and the ATAC server;

- one-way encryption of application passwords with SHA2_256 hash algorithm; implementation of the password change of agents with expiration of three months;

- database access log; the anonymous storage of the data of the “Details of Movements” function has been aligned with that of

the dbo E-MulteS table, therefore also in this case, after 60 days, the data is made anonymous;

- the use of the E-MulteS application was adapted to the use of the https protocol already during inspections. In fact, from the minutes of the XXth it is noted that access has already been set with the https protocol;

- the access authentication system has been implemented, passwords are encrypted and the length has been increased to 8 characters;

- the system has been implemented with a log that allows both to track the Auxiliary who has made a specific fine, and to track the response that is given to the Traffic Auxiliary following a query by license plate. It is confirmed that the Auxiliaries can access only in reading and only the data of the current day;

- the log has also been implemented which allows the tracing of accesses to the Data Base carried out by the System Administrators, both for successful accesses and for unsuccessful attempts;

- only some back-office operators of the Parking and Parking Division have access - for the necessary management of high penalties - to all the data present in the dbo E-MulteS (fined vehicle number plate, date, time, place, Auxiliaries of the Traffic Detector) but they see the plate data for the last 60 days in clear text. After 60 days, the plate data is made anonymous. Access to the EmulteS dbo of back-office operators is subject to specific authorizations and is not allowed to Traffic Auxiliaries ";

- Atac has adopted a new way of managing the programming of services regarding the control over the territory carried out by the Traffic Auxiliaries. Through a new platform owned by ATAC (GTP-Sosta). In fact, "the aforementioned platform is able to assign daily routes to be checked on the basis of predetermined weekly frequencies in compliance with the quality objectives indicated in the Service Contract - through GTP-Sosta, in automated mode, the Traffic Auxiliaries are therefore assigned to the "walkways" (service routes), so that the teams are always made up of different Traffic Auxiliaries for different walkways but still belonging to the same shift and garrison. The adoption of this safety measure excludes the possibility that the Traffic Auxiliaries always travel the same route assigned to them to check the stops and thus can always detect the same number plates of the cars that eventually should always park in the same place / area ".

Roma Capitale has not provided information about the adequate measures to ensure that only the necessary data are processed, with particular reference to the definition of the retention times of personal data, nor does it appear to have given the relevant instructions to Atac s.p.a.

3. Outcome of the preliminary investigation

According to the regulations on the protection of personal data, public entities (such as Roma Capitale) can process data only if necessary "to fulfill a legal obligation to which the data controller is subject" or "for the execution of a task of public interest or connected to the exercise of public powers vested in the data controller "(art. 6, par. 1, lett. c) and e) of the Regulation). In this context, the regulation of parking and paid parking is part of the institutional activities entrusted to local authorities.

Even in the presence of a legal prerequisite, in any case, the data controller is still required to respect the principles of data protection, including those of "lawfulness, correctness and transparency", "limitation of conservation" and " integrity and confidentiality "on the basis of which the data are" processed in a lawful, correct and transparent manner towards the interested party "," kept in a form that allows the identification of the interested parties for a period of time not exceeding the achievement of the purposes for which they are processed "and" processed in such a way as to guarantee adequate security of personal data, including the protection, by means of adequate technical and organizational measures, from unauthorized processing "(Article 5, paragraph 1, letter a) , e) and f), of the Regulation).

3.1 Information for interested parties

From the documentation in the documents and as declared during the inspection (attachment 5 of the XX report), from the date of activation of the service in question (XX) to the date on which the owner Roma Capitale declared that he had made the information interested parties (XX, note of XX, annex 10-bis and annex 17) it is ascertained that the information is not provided to the interested parties.

Therefore, the processing appears to have been carried out by Roma Capitale in violation of the obligation that requires the data controller to provide the data subjects with prior information, in accordance with the provisions of Articles 12 and 13 of the Regulation, also in compliance with the "principle of transparency" (Article 5, letter a) of the Regulation).

3.2. The principles of data protection by design and data protection by default

According to the Regulation, it is up to the data controller, in this case Roma Capitale, "taking into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing, as also risks having different probabilities and gravity for the rights and freedoms of natural persons "to put in place adequate technical and organizational measures to ensure that, by default, only the personal data necessary for each specific purpose of the processing are processed. This obligation applies to the quantity of personal data collected, the scope of the processing, the

retention period and accessibility "(Article 25, paragraphs 1 and 2).

In the light of the declarations made, however, it appears that Roma Capitale (minutes XX) has not defined the retention times of the personal data collected nor has it given precise instructions to Atac s.p.a ..

Since "adequate measures have not been adopted to ensure that only the necessary data are processed, with particular reference to the definition of the retention times of personal data", the violation of the principles of "retention limitation" and "data protection from design and data protection by default "pursuant to art. 5, par. 1, lett. e) and 25 and of the Regulations.

3.3. Failure to define the role of external parties involved in the treatment

For the purposes of compliance with the legislation on the protection of personal data, it is necessary to precisely identify the subjects who, for various reasons, can process personal data and clearly define their respective powers, in particular that of owner and manager of the treatment and subjects who operate under their direct responsibility (Article 4, paragraph 1, point 7 of the Regulations).

As previously clarified by the Guarantor, the owner, in this case Roma Capitale, is the subject on whom the decisions regarding the purposes and methods of processing the personal data of the interested parties fall as well as a "general responsibility" on the treatments put in place (see art. 5, par. 2 so-called “accountability” and 24 of the Regulations), even when these are carried out by other subjects “on its behalf” (cons. 81, art. 4, point 8) and 28 of the Regulations; cf. also provision no. 81 of 7 March 2019, doc. web 9121890; provision no. 160 of 17 September 2020, doc. web 9461168).

The relationship between owner and manager must be governed by a contract or other legal act, stipulated in writing which, in addition to mutually binding the two figures, allows the owner to give instructions to the manager and provides, in detail, which is the subject matter governed. , the duration, the nature and the purposes of the processing, the type of personal data and the categories of data subjects, the obligations and rights of the owner. The Data Processor is therefore entitled to process the data of the interested parties "only on the documented instruction of the owner" (Article 28, paragraph 3, letter a) of the Regulation).

The Regulation also governed the obligations and other forms of cooperation to which the data controller is required when acting on behalf of the owner and the scope of their respective responsibilities (see articles 30, 33, par. 2 and 82 of the Regulation) .

Based on art. 24 of the Regulation, taking into account the nature, scope, context and purposes of the processing, as well as

the risks with different probability and severity for the rights and freedoms of natural persons, it is primarily up to the data controller to put adequate technical and organizational measures are in place to guarantee, and be able to demonstrate, that the processing is carried out in accordance with the Regulations. These measures must also be reviewed and updated as necessary.

During the investigation it emerged that Roma Capitale failed to define the role of Atac s.p.a. and Flowbird s.r.l. (formerly Parkeon s.r.l.) before the start of the processing of personal data, in violation of art. 28 of the Regulation.

In relation to the profiles regarding the protection of personal data, it is noted that the resolutions of Roma Capitale (no. XX of the XX and no. XX of the XX), with which the service in question was entrusted to Atac s.p.a, did not the specific characteristics of the legal act that defines the role of the Manager, as they do not contain the elements provided for by art. 28 of the Regulation (see spec. Par. 3).

The failure to define the relationship with external parties (Atac s.p.a. and Flowbird s.r.l.) involved in the processing, - without prejudice to the assessments regarding the lawfulness of the processing carried out by the companies, which will be the subject of independent proceedings - resulted in the violation of art. 28 of the Regulations by Roma Capitale.

3.4 Data security

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 ".

As previously clarified by the Guarantor, due to the "general responsibility" of the data controller (Article 5, paragraph 2 of the Regulation) the same is required to "implement adequate and effective measures [and ...] demonstrate the compliance of the processing activities with the [...] Regulation, including the effectiveness of the measures "(cons. 74, articles 4, point 7) and 24 of the Regulation) and, in this context, for the purpose of preparing the technical and organizational measures that meet the requirements established by the Regulations, the data controller may also have recourse to a Manager to carry out some

processing activities, to whom he / she gives specific instructions, also from the point of view of security (see cons. 81 of the Regulations; see provision no. 160 of 17 September 2020; provision no.49 of 11 February 2021, web doc. 9562852), supervising the work of the same.

The methods of processing ascertained highlight the failure by Roma Capitale to adopt appropriate technical and organizational measures to guarantee a level of security adequate to the risks presented by the processing, nor do any specific instructions appear to have been given in this regard to the responsible for the treatment, with consequent violation of art. 32 of the Regulation.

4. Conclusions

In light of the aforementioned assessments, it is noted that the statements made by Roma Capitale, as data controller, in the defensive writings sent to the Guarantor whose truthfulness you may be called to answer pursuant to art. 168 of the Code although worthy of consideration, they do not allow to overcome the findings notified by the Office with the act of initiation of the procedure and are insufficient to allow the filing of this procedure, however, none of the cases provided for by the art. 11 of the Guarantor Regulation n. 1/2019.

From the checks carried out on the basis of the elements acquired, also through the documentation sent by the data controller, as well as from the subsequent evaluations, the non-conformity of the treatments carried out by Roma Capitale concerning the data collected through the new parking meters installed in the area was ascertained.

The violation of personal data, object of the investigation, took place in full force of the provisions of the Regulation and the Code, as amended by Legislative Decree No. 101/2018, and therefore, in order to determine the regulatory framework applicable under the time profile (art. 1, paragraph 2, of the l. 24 November 1981, n. 689), these constitute the provisions in force at the time of the committed violation, which took place starting from the month of XX.

Therefore, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by Roma Capitale is noted, as it occurred in a manner that did not comply with the general principles of processing, in the absence of suitable information and appointment of the managers of the treatment, as well as in the absence of technical and organizational measures suitable to guarantee a level of security adequate to the risk presented by the treatment, in violation of art. 5, 12, 13, 25, 28 and 32 of the Regulation.

The violation of the aforementioned provisions makes the administrative sanction applicable pursuant to art. 58, par. 2, lett. i),

and 83, para. 4 and 5, of the same Regulation, as also referred to by art. 166, paragraph 2, of the Code.

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

As regards the security measures implemented to date, taking into account the statements made by the data controller, some critical issues remain.

First of all, the adoption of the new GPT system as an organizational measure aimed at precluding that the single auxiliary does not exercise frequent (in a physical sense) control over the same plates due to the rotation in terms of zones / districts does not solve the critical issues, already object of dispute, relating to the absence of recording functionality of the work of individual users nor, even less, of identifying anomalous behavior (through specific alerts).

In relation to storage times, the documentation in the file shows that the choice of "one-way encryption of plates older than 60 days with MD5 hash algorithm" was made independently by the data controller, Atac s.p.a., who did not receive specific instructions, in this regard, by the Municipality of Rome. It is not clear the reasons why Atac s.p.a has chosen to make "unintelligible" the data of the license plates for which the payments date back to a period of more than 60 days, and in any case, the security measure implemented cannot be considered suitable for the reasons indicated below.

The storage for an indefinite time of the computer fingerprints of the values of the number plates calculated by applying the MD5 hash function, referred to as "one-way encryption" for the "anonymization" of the data, is not very reliable as it allows easy identification and correlation, which represent two of the main risks affecting these techniques.

More precisely, starting from a plate it is possible to calculate its hash and search for all occurrences in the database, thus allowing the historical reconstruction of all payments made, and consequently of all the stops made.

For these reasons, also taking into account the size of the set of possible plates (consisting of two letters, three numbers and two letters), the computational simplicity of the algorithm used and the scarcity of the technological resources necessary to trace the clear data, the technique used is not suitable

It is therefore considered necessary to implement the technical security measures - giving precise and detailed instructions to this effect to the data controller, Atac s.p.a - which allow the traceability of the operations carried out (application logs) by users on personal data in order to verify ex post the work of its employees with respect to the computerized processing of a large volume of data relating to a large number of data subjects that can potentially lend themselves to fraudulent uses to their detriment, allowing to detect the state of absence from home or the presence in a specific area of the city in a given period of

time. It is also considered necessary to define the retention times of the data relating to the plates and the consequent technical measures to protect the stored data, bearing in mind that the robustness of the measures is directly proportional to the length of the storage period.

Having said that, it is considered necessary, pursuant to art. 58, par. 2, lett. d), of the Regulations, to order Roma Capitale, within thirty days of notification of this provision, to adopt, in agreement with the data controller:

- recording functions (application logs) of the work of individual users, whether they are system administrators or back office operators and traffic auxiliaries, and functions for identifying anomalous behavior (through specific alerts) in order to verify ex post the the work of its employees with respect to the computerized processing of a large volume of data relating to a large number of interested parties;
- suitable security measures to protect the information stored consistently with the maximum retention times chosen.

Pursuant to art. 157 of the Code, Roma Capitale must also communicate to this Authority what initiatives have been undertaken in order to implement the provisions of this provision and in any case to provide adequately documented feedback, within thirty days of notification of this provision.

6. Adoption of the injunction order for the application of the pecuniary administrative sanction and ancillary sanctions (articles 58, par. 2, lett. I and 83 of the Regulation; art. 166, paragraph 7, of the Code)

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

In this regard, taking into account art. 83, par. 3, of the Regulation, in 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 purposes of applying the sanction, it was considered that the processing of personal data collected through the new

parking meters, operational starting from the month of XX, is still ongoing and has potentially affected all those who use the paid parking service on the municipal area. As of the twentieth century, 8,600,000 data relating to the stops made by vehicles have already been recorded in the system created by Atac s.p.a., on behalf of Roma Capitale.

This processing took place in the absence of suitable information, in violation of the principle of "lawfulness, correctness and transparency" pursuant to art. 5, lett. a), 12 and 13 of the Regulation, in the absence of identification of the maximum retention terms of the collected data, in violation of the principles of "retention limitation" and "data protection by design and data protection by default" of referred to in Articles 5, lett. e) and 25 of the Regulations, in the absence of definition of the role, as "data processors", of the subjects involved in the same in violation of art. 28 of the Regulations and in the absence of adequate technical and organizational measures in violation of the principle of "integrity and confidentiality" pursuant to art. 5 lett. f) and 32 of the Regulations.

Account was taken of the type of personal data being processed and the fact that Roma Capitale has adopted some measures in order to remedy the violation and mitigate its possible negative effects, giving the information to the interested parties and defining the role played by Atac s.p.a. and Flowbird s.r.l. in the treatment under consideration; and the non-malicious behavior of the data controller has also been acknowledged.

On the other hand, however, the "general responsibility" of the processing, placed in the hands of Roma Capitale, as the data controller, has been taken into account, which can also use a person in charge to carry out some processing activities, provided that he gives specific instructions , also from the point of view of safety. In this regard, however, the insufficiency or inadequacy of some technical and organizational measures adopted during the procedure emerged, which resulted in the need to prescribe the corrective measures referred to in paragraph 5.

It was considered that the violation was brought to the attention of the Authority through a report. Account was also taken of the numerous violations detected by the Authority against Roma Capitale in the context of previous proceedings (provisions no. XX of the XX, no. XX of the XX, no. XX of the XX and no. XX of the XX) also concerning the violation of the same provisions of the Regulations.

Due to the aforementioned elements, assessed as a whole, it is deemed necessary to determine pursuant to art. 83, par. 2 and 3, of the Regulations, the amount of the pecuniary sanction, provided for by art. 83, par. 5, lett. a) of the Regulations, to the extent of Euro 800,000.00 (eight hundred thousand) for the violation of Articles 5, 12,13, 25, 28 and 32 of the Regulation as a

pecuniary administrative sanction deemed effective, proportionate and dissuasive pursuant to art. 83, par. 1, of the same Regulation.

Taking into account the high number of data subjects involved in the processing in question and the lack of adoption of adequate technical security measures, it is believed that the additional sanction of the publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Guarantor Regulation n. 1/2019.

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

WHEREAS, THE GUARANTOR

the unlawfulness of the processing carried out by Roma Capitale for the violation of Articles 5, 12, 13, 25, 28 and 32 of the Regulation, in the terms set out in the motivation,

ORDER

in Roma Capitale, in the person of the pro-tempore legal representative, with registered office in Piazza del Campidoglio, n. 1, Rome - C.F. 02438750586 - to pay the sum of Euro 800,000.00 (eight hundred thousand) as a pecuniary administrative sanction for violations of Articles 5, 12, 13, 25, 28 and 32 of the Regulations; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the sanction imposed;

INJUNCES

in Rome Capital

a) to pay the sum of € 800,000.00 (eight hundred thousand), in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, according to the methods indicated in the annex, within thirty days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the l. n. 689/1981;

b) pursuant to art. 58, par. 2, lett. d) of the Regulations, to conform the processing to the provisions of the Regulations, adopting the corrective measures indicated in paragraph 5 of this provision, no later than 30 days from the date of receipt of the same. Failure to comply with an order formulated pursuant to art. 58, par. 2, of the Regulations, is punished with the administrative sanction referred to in art. 83, par. 6, of the Regulations;

c) pursuant to art. 58, par. 1, lett. a), of the Regulations, and of art. 157 of the Code, to communicate which initiatives have

been undertaken in order to implement the provisions of the aforementioned par. 5, and in any case to provide adequately documented feedback, no later than 30 days from receipt of this provision. Failure to respond to a request made pursuant to art. 157 of the Code is punished with an administrative sanction, pursuant to the combined provisions of art. 83, par. 5, of the Regulation and 166 of the Code;

HAS

the publication of this provision on the website of the Guarantor, pursuant to art. 166, paragraph 7, of the Code and art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019;

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 no. 150/2011, against this provision, it is possible to appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the applicant resides abroad.

Rome, July 22, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei