

SEE ALSO NEWSLETTER OF MARCH 29, 2021

[doc. web no. 9562831]

Order of injunction against Roma Servizi per La Mobilità S.r.l. - February 11, 2021

Register of measures

no. 48 of 11 February 2021

## THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

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

HAVING REGARD TO 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 the national legal system to the Regulation (hereinafter the "Code");

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

HAVING REGARD to the documentation in the deeds;

GIVEN the observations of the Office formulated by the Secretary General pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, in [www.gpdp.it](http://www.gpdp.it), doc. web no. 1098801;

SPEAKER Prof. Geneva Cerrina Feroni;

WHEREAS

1. Premise.

From some press reports, published in December 2018, and from a report presented to the Authority, it was learned that the

permits for access and parking in the limited traffic areas ("Z.T.L.") of Rome Capital, to be displayed on vehicles, show on the title page a so-called QR code, which allows anyone, through the use of a generic application for mobile devices (mobile app) capable of decoding its content, to access personal data relating to the holder of the Z.T.L. or its user.

## 2. The preliminary investigation.

In response to the Office's request for information, Roma Capitale provided a reply (note prot. n. XX of the XX), through the designated data controller, Roma Servizi per la Mobilità S.r.l. (hereinafter, "Roma Servizi").

Specifically, the legal representative of Roma Servizi represented, among other things, that:

"carries out assistance and support activities on behalf of Roma Capitale in the management of mobility services. In particular and to the extent of interest, Roma Capitale [it] has entrusted it on its own [...] behalf with carrying out the activities related to the issue and renewal of permits for access, circulation and parking in restricted traffic areas [...], the basic discipline of which is contained in the resolution of the City Council of Rome Capital n. 183 of 16 January 1996";

"in the activities of issuing permits Z.T.L. those consisting in the printing and issuing of the related stamps are included";

"a new type of mark in paper format bearing a QR code containing the identification information of the authorization", as well as

"the related model", were adopted with executive decisions nos. XX and XX of the XX and XX of the Mobility and Transport Department of Rome Capital, and "the current format has been operational since 1 December 2016";

the information reported "in the clear" (i.e. not encoded in the QR code) on the mark, intended to be displayed, concerns: the type of authorization (e.g. access, parking, unloading of goods, etc.), the vehicle number plate, the number of the permit and the temporal validity. The QR code, on the other hand, shows: the category of the applicant (e.g. domiciled, goods distributor, parking space owner, etc.), the company or institutional reason or denomination (in the case of a vehicle belonging to a legal person) or the name and surname (in the case of a natural person) of the permit holder, as well as the name and surname of the user of the same;

"all the information shown on the side of the sign intended to be displayed, some of which is visible only with a QR code, appears to be necessary to allow road activities carried out by the competent authorities aimed at checking that the permits are used in compliance with DGC 183/ 96".

From the preliminary official investigations it has been verified that the QR codes, reported in the Z.T.L. – ten of which were produced by Roma Servizi during the investigation, with note prot. no. XX of XX – encode web addresses in URL format like

<https://permessiweb.atac.roma.it/VerifyPermit.aspx?PID=nnn&Source=xyz>, which include two parameters: the first (called "PID" ), identifier of the single permit, consisting of a numerical sequence, the second (called "Source"), which indicates the possible temporary validity of the permit.

Therefore, it was ascertained that with a generic mobile app, capable of decoding the content of the aforementioned QR codes, anyone could have connected to the web address of the Z.T.L. permit verification service, thus accessing the data relating to the single permit, including which: the company or institutional name (e.g. Rome Police Headquarters, elementary school) or the name and surname (in the case of a natural person) of the permit holder, the name and surname of the user of the permit, the category of the applicant (e.g. craftsman, night worker), as well as the license plate of the authorized vehicle. It was also verified that, by modifying the value of the parameter called "PID" (simply increasing or decreasing the numerical identifier of the permit) within the web address of the verification service, it was also possible to view the personal data relating to other Z.T.L. permits, even if the corresponding QR code is not available. This happened because the online permit verification service Z.T.L. it was freely accessible, not being protected by any authentication procedure.

In relation to these violations, the notification provided for by art. 166, paragraph 5, of the Code, of the violation of art. 32 of the Regulation, communicating the start of the procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation, inviting the entity to send written defenses or documents (art. 166, paragraphs 6 and 7, of the Code; as well as art. 18, paragraph 1, of law n. 689 of 24 November 1981).

With note prot. no. XX of the XX, Roma Servizi sent its defense writings to the Guarantor in relation to the notified violation, declaring, in particular, that:

- "in his capacity as data controller, he does not appear to have received specific instructions regarding any technical security measures to be implemented with regard to the QR code";
- "as regards the parameters of the nature, object, context and purpose of the processing, in the absence of more stringent indications from Rome Capital on this point, they correspond to what is necessary to allow road activities conducted by the competent authorities and aimed at verifying that the permits are used in compliance with [...] executive determination XX above;
- "as regards the risk for the rights and freedoms of natural persons, the impact for data subjects deriving from the possible loss of confidentiality of personal data is deemed to be classified as low. Therefore, the implementation of the QR Code can

already be qualified in itself as a first security measure to protect the confidentiality of the data subjects";

- that I have temporarily suspended the online Z.T.L. permit verification service by reading the QR code starting around 2.30 pm on 2 April 2019 and intending to implement an "access control system to the public verification page for which, in the event of web calls to this page, a filter will operate with redirection to an authentication page through credentials of subjects who need to view the data for service reasons".

On 17 May 2019, the hearing requested by the company pursuant to art. 166, paragraph 6, of the Code, during which it was declared, among other things, that the application development activities of the aforementioned access control system "were completed on 13 May 2019, the date from which the verification of the ZTL permits has been reactivated" (see also note prot. XX of XX), highlighting that "for reasons of continuity of service, the suspension [of the same] could not go on any longer and that a buffer solution has been adopted which will be improved also on the basis of the results of the internal audit initiatives and the vulnerability assessment and penetration test activities entrusted to specialized third parties".

The company also declared that, at present, access to the Z.T.L. is allowed only to authorized subjects with "personal authentication credentials, consisting of a username and password" and that "access to the ZTL permit verification service is permitted to [the company's] personnel employed in permit management activities ZTL as well as to the persons in charge of road control activities (Local Police of Rome Capital and State Police) and of management of the sanctioning procedure (Prefecture of Rome)".

It also emerged that the passwords relating to the users of the authorized parties "do not [must] satisfy specific complexity rules and do not [n] have a predefined expiration date" and that "mechanisms for the automatic blocking of credentials have not been envisaged in case of repeated failed authentication attempts". In this regard, the company represented that "actions are planned for the future to increase the level of security of the system also on the basis of the results of the audits already carried out by the Data Protection Manager".

### 3. Outcome of the preliminary investigation.

Pursuant to art. 28 of the Regulation, the owner can also entrust a treatment to data controllers who present sufficient guarantees with regard to the implementation of technical and organizational measures suitable to guarantee that the treatment complies with the regulations on the protection of personal data (cf. art. 29 of the previous Code).

Although the data processor is required to process the data in accordance with the instructions given by the data controller,

certain obligations are, however, also placed directly on the manager himself.

As regards, in particular, the security of the treatment, the 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, object of the context and 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 guarantee a level of security appropriate to the risk" and that "in assessing the adequate level of security, particular account is taken of the risks presented by the processing which derive in particular [...] from the unauthorized disclosure or access, in an accidental or illegal manner, to the personal data transmitted, stored or in any case processed" (see also articles 31 and following of the previous Code).

From the checks carried out on the basis of the elements acquired, also through the documentation sent by the bodies involved, as well as from the subsequent assessments, the Office ascertained the non-compliance - with regard to both the previous legislation (or the Code, in the text prior to the amendments made by Legislative Decree 10 August 2018, No. 101), and the current regulations on data protection - of the processing in question, carried out starting from 1 December 2016 and continued until April 2019.

It should be noted first of all that, as ascertained by the Authority in the context of the overall investigation, the personal data relating to the holders and users of the Z.T.L. displayed on the vehicles were made accessible to an indeterminate audience of third parties - who could read the QR codes shown in the permits through a generic mobile app, available on common smartphones capable of decoding the content - thus giving rise to a "dissemination" of personal data (cf. art. 2-ter, paragraph 4, letter b) of the Code).

It was also verified that by accessing the web address of the permit verification service and modifying the value of the "PID" parameter within it, it was possible to view the personal data relating to Z.T.L. permits. of subjects to whom the permit had been issued, even though the corresponding QR code shown in the permit issued to them was not available.

From the aforementioned assessment, it emerged that, starting from 1 December 2016 (the date from which the paper format bearing a QR code and the relative online verification service is operational for Z.T.L permits), the dissemination of the aforementioned personal data it occurred as a result of the failure to adopt suitable technical and organizational measures to guarantee a level of security adequate to the risks presented by the processing, such as the unauthorized dissemination of personal data and access to them, accidentally or illegally.

In the light of the above, Roma Servizi has been held responsible for the failure to adopt suitable technical and organizational measures to guarantee a level of security adequate to the risks presented by the processing, creating the conditions for the occurrence of the illicit dissemination of personal data, in violation of the art. 32 of the Regulation.

#### 4. Conclusions.

In the light of the assessments referred to above, it should be noted that the statements made by the data controller in the defense writings □ the truthfulness of which may be called upon to answer pursuant to art. 168 of the Code □ although worthy of consideration, do not allow the findings notified by the Office to be overcome with the act of initiation of the proceeding and are insufficient to allow the dismissal of the present proceeding, since none of the cases envisaged by the art. 11 of the Regulation of the Guarantor n. 1/2019.

For the determination of the applicable rule, in terms of time, the principle of legality pursuant to art. 1, paragraph 2, of the law no. 689/1981, pursuant to which the laws that provide for administrative sanctions are applied only in the cases and within the times considered in them". This determines the obligation to take into consideration the provisions in force at the time of the committed violation, which in the case in question - given the permanent nature of the disputed offense - must be identified in the act of cessation of the unlawful conduct, which occurred after 25 May 2018, date on which the Regulation became applicable. In fact, the preliminary investigation documents revealed that the unlawful processing lasted until April 2019.

The preliminary assessments of the Office are therefore confirmed and the illegality of the processing of personal data carried out by Roma Servizi is noted, as it took place in a manner that does not comply with the general principles of processing, in the absence of an appropriate legal basis, as well as in the absence of suitable technical and organizational measures to guarantee a level of security adequate to the risk presented by the treatment, in violation of art. 32 of the Regulation.

The violation of the aforementioned provision renders the administrative sanction applicable pursuant to articles 58, par. 2, lit. i), and 83, par. 4 of the same Regulation, as also referred to by art. 166, paragraph 2, of the Code.

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

Taking note of what emerged during the hearing and of the measures already introduced, taking into account the fact that the Z.T.L. was exposed on the public network and the consequent risks presented by the treatment, which derive in particular from the possibility of access, accidentally or illegally, to the personal data processed, it is necessary to order Roma Servizi, pursuant to art. 58, par. 2, lit. d), of the Regulation, to modify, within and no later than 30 days from the date of receipt of this

provision, the computer authentication system used in the context of the Z.T.L. permit verification service, in compliance with art. 32 of the Regulation, adopting, in agreement with the data controller, the technical and organizational measures indicated below or other similar measures, also taking into account any initiatives undertaken in this regard over time, which in any case guarantee an adequate level of security the risks presented by the treatment concerning:

a) the ability to ensure the confidentiality of the data processed, making sure that the passwords relating to the users of the authorized subjects are no less than eight characters long and are subjected to an automatic quality control that prevents the use of "weak" passwords " and that the same passwords are changed at least on first use;

b) the ability to effectively counter brute force cyber attacks on the online authentication system, also by introducing limitations on the number of unsuccessful authentication attempts.

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

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

In this regard, in the present case, the violation of the aforementioned provision is subject to the application of the administrative fine provided for by art. 83, par. 4, of the Regulation.

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

In relation to the aforementioned elements, the extended period of time in which the violation took place was assessed, as well as the fact that it affected a large number of interested parties. Furthermore, there are previous violations of the relevant Regulations committed by Roma Servizi.

On the other hand, it was taken into account that, although the violation in question was brought to the attention of the Authority through various press reports published in December 2018 and through a subsequent report, Roma Servizi took

steps to remedy the violation and mitigate the possible negative effects, introducing some initial technical and organizational measures pursuant to art. 32 of the Regulation, having been, in any case, considered the non-malicious behavior of the violation.

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction, in the amount of 60,000 (sixty thousand) euros for the violation of art. 32 of the Regulation, as a pecuniary administrative sanction deemed effective, proportionate and dissuasive pursuant to art. 83, par. 1, of the same Regulation.

In relation to the specific circumstances of the present case, it is also believed - also in consideration of the high number of interested parties involved in the unlawful dissemination, which lasted for more than a year - that the accessory sanction of publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7, of the Code and art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019.

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

#### ALL THIS CONSIDERING THE GUARANTOR

notes the illegality of the processing carried out by Roma Servizi for the violation of the art. 32 of the Regulation, in the terms referred to in the justification;

#### ORDER

in Rome Servizi per La Mobilità S.r.l., in the person of its pro-tempore legal representative, with registered office in Via Di Vigna Murata, 60 - 00143 Rome (RM) – Tax Code 10735431008 – to pay the sum of 60,000 (sixty thousand) euros as an administrative fine for the violations referred to in the justification; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the fine imposed;

#### ENJOYS

- a) to Roma Servizi to pay the sum of 60,000 (sixty thousand) – without prejudice to the provisions of the aforementioned art. 166, paragraph 8, of the Code - according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the law no. 689/1981;
- b) to Roma Servizi, pursuant to art. 58, par. 2, lit. d), of the Regulation, to conform the treatments to the provisions of the Regulation, adopting the corrective measures indicated in paragraph 5 of this provision, within and 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 Regulation, is punished with the administrative sanction pursuant to art. 83, par. 6, of the Regulation;

c) to Roma Servizi, pursuant to art. 58, par. 1, lit. a), of the Regulation, and of the art. 157 of the Code, to communicate, by providing adequately documented feedback, within and no later than 30 days from receipt of this provision, the initiatives undertaken to bring processing into line with the provisions of the aforementioned paragraph 5. Failure to respond to a request made pursuant to the 'art. 157 of the Code is punished with an administrative sanction, pursuant to the combined provisions of articles 83, par. 5 of the Regulation and 166 of the Code;

HAS

the publication of this provision on the Guarantor's website, pursuant to art. 166, paragraph 7, of the Code and of the 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, lit. u), of the Regulation, of the violations and of the measures adopted in accordance with art. 58, par. 2, of the Regulation.

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

Rome, 11 February 2021

PRESIDENT

Station

THE SPEAKER

Geneva Cerrina Feroni

THE SECRETARY GENERAL

Matthew