[doc. web n. 9733053]

Order injunction against Ica s.r.l. - December 2, 2021

Record of measures

n. 419 of 2 December 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;

Rapporteur Dr. Agostino Ghiglia;

1. Introduction

From a complaint submitted to the Authority in the month of XX, it emerged that the online payment service for the fines of the Municipality of Collegno had been configured in the absence of suitable security measures pursuant to art. 32 of the Regulation. According to the complainant, in fact, the configurations adopted allowed anyone to know the personal data of

citizens who had been fined and who could make use of the aforementioned payment service. In particular, “until the twentieth century it was possible to access personal information relating to fines. To carry out the violation, simply indicate: a report number (the reports are sequentially numbered) and a date (consistent with the numbering of the reports) without indicating the plate. By doing so, it was possible to acquire the personal data of the interested parties such as: the license plate, the time at which the infringement was detected, the type of infringement, the amount to be paid and the photograph of the car ".

2. Preliminary activity

In relation to the case, an investigation was initiated, during which it emerged that the Municipality of Collegno - the data controller - has entered into with ICA s.r.l. (hereinafter, the company) a contract for the assignment of the management service of violations of the Highway Code, as well as administrative violations other than the Highway Code of competence of the body, including ordinary and compulsory collection activities; it also took steps to regulate the relationship with the company, pursuant to art. 28 of the Regulation, with an "deed of appointment as an external data processing manager".

In response to the Authority's request for information (prot. Note no. XX of the XX) the company, with a note of the XX, stated, among other things:

"To be" contractor from the Municipality [...] of the support service for the assessment and collection of administrative penalties for violations of the Highway Code ";

“The service includes the supply to the Municipal Police Command of specific management software and the related maintenance and updating services […]. This is the "Vigilando" software, installed on the server dedicated to the service at the "Consortium for the Information System" C.S.I. Piedmont ";

"The use of the cloud service of C.S.I. it took place, in agreement with the Municipality, “in variation to the provisions of the specifications […] for which the server had to be physically located at the Municipality”;

"The" Vigilando "software has an interface to users; this is the "Payment Portal" web application, through which the interested party can access the data in their reports and make the related payment. In particular, in relation to each report it is possible to access the following data, [...]: - amount of the report - any detection photos, in which the driver is never visible but only the license plate - license plate and model of the vehicle - law violated "while" in the event that the report does not refer to a vehicle equipped with a license plate, the data accessed through the portal are the same except for the license plate ";

"Each local body, as Data Controller, indicates to the writer how users can access the payment portal. The Municipality of

Collegno has requested a double accreditation system […]: - insertion of year, date and n. report for access to violations affecting pedestrians - entry of the aforementioned data and in addition of the license plate number for those relating to motor vehicles. In practice, the Command, by entering the reports in the system, evaluates the fields "S" (Italian plate), "N" (foreign plate) or "A" or "null" (no plate). In the first two cases, the software makes access subject to also entering the license plate number ";

“Except that the software no longer performed this operation; it no longer linked the “license plate” requirement to the S and N values; hence the possibility to access without indication of the license plate, even where present. The functionality must have been lost in the software updates (or in the installation on the CSI Piemonte server), and ICA was not aware of this until the 20th, when the Municipality made known the report of the [complainant] ";

“It should be noted that in all the other contracts for the management of CDS reports, the Municipalities have requested a single accreditation system, in which the fields to be entered are always the same and do not vary according to the type of report. That of Collegno is therefore a singularity with respect to the normal functioning of the application, which required an ad hoc intervention. The writer is aware that this does not justify what happened, but at least provides an explanation ";

"Upon receipt of the user's report on XX, the writer immediately restored the above functionality. So from the early afternoon of that day, access was again subject to entering the license plate number. The lack of internal coordination between the IT services and the technical contact person at the Municipality meant that the latter, carried out the verification test in the late evening of the same day, reported to the Municipality that the access system required the insertion of the number plate, without knowing that this depended on the maintenance intervention. On the 20th, a joint test was carried out between ICA and the Municipality through which it was certified that access was subject to the insertion of the license plate ".

From the documentation sent, therefore, it was ascertained that, probably due to a "software update", the insertion of the "License plate" field was no longer mandatory for access to the data of the reports processed as part of the payment service of the fines, unlike what was previously set. Consequently, by filling in only the "Year", "Report" and "Date of violation" fields, anyone could have access to personal data of third parties. Similarly, with regard to other administrative violations (eg pedestrian violations), it has been ascertained that to access the data of the online report it is necessary to fill in only the "Year", "Report" and "Date of violation" fields, without entering further confirmation data not easily predictable and known only by the offender.

Therefore, with a note dated XX (prot. No. XX), 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 company to produce defensive writings or documents to the Guarantor or to ask to be heard by the Authority (art.166, paragraphs 6 and 7, of the Code; as well as art.18, paragraph 1, of law n. 689 of 11/24/1981). With the aforementioned note, the Office found that the company carried out the processing of the personal data in question without having adopted appropriate security measures to ensure the confidentiality of the data processed on a permanent basis, in violation of Articles 5, par. 1, lett. f), and 32 of the Regulation.

With a note of the twentieth, the company presented the defense briefs, declaring:

"From the verification carried out following the notification of the violation, it appears that the Web service" Portal Payments Vigilando "was installed on the CSI Piemonte server on XX [...] After that date, the Portal had only one update on XX, which concerned an aspect unrelated to the access credentials, but which "could have inserted an application bug in the portal that allows the user to carry out searches without entering the license plate number [...] In this sense, the temporal proximity would also pose between the update and the user's report, together with the fact that no report had previously been received by the Entity or the writer regarding this malfunction. If this is not the case, the start of the processing in violation of the security obligations should be traced back to the date of the XXth, ie the moment of the first installation of the Portal containing the bug ";

“As regards the reports concerning the vehicles, the following data is accessed via the payment portal […]: - amount of the report - any detection photos, in which the driver is never visible but only the license plate. - license plate and model of the vehicle. - article of law violated. In particular, in the portal: - there is no copy of the report, from which it would be possible to access additional information. - The name of the owner of the vehicle or of the transgressor is not indicated. Therefore, the inadequate level of security that was determined as a result of the malfunction allowed access to data: - which are not of the nature of “particular” data or those relating to criminal convictions and offenses. - which are not immediately associated with an interested party, except through a paid search at the ACI. It should also be noted that as a result of the bug it was possible to access the aforementioned data with a random search (ie starting from a record number known on a certain date, it was possible to indicate progressive numbers) and not targeted, ie aimed at acquiring certain information " ;

"Moreover, it appears that the bug (not immediately perceptible by the user, given that the" plate "field was still present in the

portal) was noticed only by the reporting person, since no other reports were received by the writer and the Data Controller";

"The reporting party also declares that he has only tried to enter progressive numbers of reports, but has not then carried out those operations (access to the PRA) necessary to trace the data of the individual positions to a specific interested party";

“It was therefore a violation of the data security obligations which: - had a negligent nature; - it was not characterized by gravity; - it had a limited duration in time; - did not prejudice the rights of the interested parties ";

"Finally, we take the liberty of reporting: - timely intervention to remedy the breach of security obligations: upon receipt of the user's report on XX, the writer immediately restored functionality. From the early afternoon of that day, access was again subject to entering the license plate number ";

"On the XX a joint test was carried out between ICA and the Municipality through which it was certified that access was subject to the insertion of the license plate";

"Simplified access to the online payment system for fines other than those involving vehicles, for which it is sufficient to enter the year, date and number of the report, depends on the fact (not specified in the information provided pursuant to art. 157 Legislative Decree 196/2003 because it is unrelated to the report) that in this case there is no processing of personal data. In fact, as shown in the attached screenshots sub docc. 5 and 6, through the payment portal you can access only the following data: - amount of the report - article of the law violated. It is therefore a mere payment instrument, where there are no data, such as the license plate, which would indirectly allow the person concerned to be traced. For this reason, the writer has not decided to object to the Data Controller's choice to proceed with a simplified access system, which responds to the need to allow users to use it easily. However, if the Guarantor deems otherwise, the writer has proposed as a possible solution that can be immediately implemented, and the Owner has declared himself available to add the so-called code to the existing access credentials. "loud". It is a serial code that is inserted in the report and therefore only those who are physically in possession of the report have the opportunity to know.

3. Outcome of the preliminary investigation

According to the regulations on the protection of personal data, public subjects 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 or related interest the exercise of public authority vested in the data controller "(Article 6, paragraph 1, letter c) and e) of the Regulation). In this context, the management of administrative violations and violations of the Highway Code is one of the institutional activities entrusted to

local authorities.

As emerged during the investigation, the processing of the data in question is carried out by the company on behalf of the Municipality of Collegno.

Pursuant to art. 28 of the Regulation, in fact, the owner can also entrust processing to third parties who present sufficient guarantees on the implementation of technical and organizational measures suitable to ensure that the processing complies with the regulations on the protection of personal data (" treatment").

Even in the presence of a condition of lawfulness, in any case, the processing of personal data must take place in compliance with the principles of data protection, including that of "integrity and confidentiality" under which the data must be " 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 or unlawful processing and from accidental loss, destruction or damage "(Article 5, par. 1, letter f). of the Regulation).

Art. 32 of the Regulation places both the owner and the manager in charge - taking into account the state of the art and the implementation costs, as well as the nature, object, context and purposes of the processing, as well as the risk - the adoption adequate technical and organizational measures to guarantee a level of safety appropriate to the risk.

As previously clarified by the Guarantor, certain obligations are also placed directly on the manager himself who, also based on the specific technical skills, must collaborate, also by showing a proactive autonomy, in the adoption of adequate measures and in the systematic verification of 'effectiveness of the same, especially if it provides services to a plurality of data controllers, which involve a large number of data subjects, as in the case in question (see provisions no.48 of 11 February 2021, web doc. . 9562831 and n. 293 of 22 July 2021, web doc. N. 9698597).

The company, precisely because of its experience in the sector, was required to constantly check the effectiveness of the measures put in place to oversee the service provided for the Municipality.

It is instead ascertained that, probably starting from the XX (date on which the "Vigilando Payments Portal" was installed on the CSI Piemonte server) or at the latest, starting from the XX (date on which an update was made) insertion of the "Plate" field was no longer mandatory for access to the data of the reports processed as part of the payment service for vehicle fines, unlike what was previously set. Consequently, by filling in only the "Year", "Report" and "Date of violation" fields, anyone could have access to personal data of third parties. This is because the data to be entered in these fields are easily predictable (eg

increasing or decreasing, in a coherent way, the number of the report and the date of the violation).

Therefore, it is ascertained that the company has not adopted technical and organizational measures suitable to guarantee a level of security adequate to the risks presented by the processing, in violation of Articles 5, par. 1, lett. f), and 32 of the Regulation.

The violation of the same articles had been contested by the Authority also with regard to the payment, through the portal in question, of the administrative violations of pedestrians. The Authority found, in fact, that in order to access the data of the online report, it is necessary to fill in only the "Year", "Report" and "Date of violation" fields, without entering additional data that are not easily predictable and only known by the offender. This profile, however, is considered superseded in the light of what the company clarified in the aforementioned note of the XXth, namely that the inclusion of the fields "year, date and number of the report, depends on the fact [...] that in this case there has been no in the presence of the processing of personal data [as…] through the payment portal only the following data is accessed: - amount of the report - article of the law violated. It is therefore a mere payment instrument, where there are no data, such as the license plate, which would indirectly allow the person concerned to be traced ".

In any case, the violation of articles 5 and 32 of the Regulations in relation to the processing of data in the context of the payment service for vehicle fines.

4. Conclusions

In light of the aforementioned assessments, it is noted that the statements made by the company □ the truthfulness of which one may be called to respond 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, as well as from the subsequent evaluations, the non-compliance of the treatments carried out by the company on behalf and in the interest of the Municipality of Collegno concerning the payment service of the fines was ascertained. relating to vehicles.

The violation of personal data, subject 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 March or at the latest, from the month of XX.

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 it occurred in the absence of technical and organizational measures suitable to guarantee a permanent level of security and adequate to the risk presented by the processing. , in violation of art. 5. par. 1. lett. f), 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.

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 individual 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 purposes of applying the sanction, it was considered that the processing of personal data collected through the online payment service for vehicle fines under the Highway Code starting from September 2019 (or, at the latest, March 2019) until 15 October 2019, and took place in the absence of effective security measures to protect it.

This violation was brought to the attention of the Authority through a complaint.

On the other hand, it was considered that the aforementioned violation lasted for a short period of time and that although it "potentially" concerns all the subjects who use the service in question, no other complaints or reports have been received that

could document that the aforementioned violation may have involved a significant number of interested parties.

It was also taken into account that the company took immediate action to remedy the violation and mitigate its possible negative effects, collaborating with the data controller, showing, in general, an attitude of broad collaboration, during the preliminary investigation. , with the Authority.

In any case, the non-malicious behavior of the violation is highlighted.

Finally, there are no previous violations of the Regulations committed by the company.

Due to the aforementioned elements, assessed as a whole, it is deemed necessary to determine pursuant to art. 83, para. 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 € 30,000 for the violation of Articles 5, par. 1, lett. f), 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 failure to adopt adequate technical security measures, it is 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 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

declares illegal the conduct of Ica s.r.l., for the violation of articles 5, par. 1, lett. f), and 32 of the Regulations, in the terms set out in the motivation,

ORDER

a Ica s.r.l., in the person of the pro-tempore legal representative, with registered office in Rome, Lungotevere della Vittoria, 9 - 00195 - C.F. 02478610583 - to pay the sum of 30,000 euros as a pecuniary administrative sanction for the violations mentioned 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 30 days, an amount equal to half of the sanction imposed;

INJUNCES

to Ica s.r.l., to pay the sum of € 30,000 (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 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, 2 December 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Ghiglia

THE SECRETARY GENERAL

Mattei