SEE ALSO: Newsletter of January 25, 2021

[doc. web no. 9525315]

Injunction against Miropass S.r.l. - December 17, 2020

Register of measures

no. 281 of 17 December 2020

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stazione, 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, concerning the protection of natural persons with regard to the processing of personal data, as well as the free movement of such data and repealing Directive 95/46/ EC, "General Data Protection Regulation" (hereinafter, "Regulation");

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national legal system to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons with regard to the processing of personal data, as well as to the free movement of such data and repealing Directive 95/46/EC (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 4/4/2019, published in the Official Gazette no. 106 of 8/5/2019 and in www.gpdp.it, doc. web no. 9107633 (hereinafter "Regulation of the Guarantor n. 1/2019");

Given the documentation in the deeds;

Given the observations made by the general secretary pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the Guarantor's office for the protection of personal data, doc. web no. 1098801;

Speaker Prof. Pasquale Station;

WHEREAS

1. The verification activity relating to the offer of public services through the "App".

During the control activity carried out on the initiative of the Authority, aimed at verifying compliance with the personal data

protection regulations put in place by public administrations in the context of the offer of public services through the so-called App, the functioning of the system called "Tupassi" provided by Miropass s.r.l. was verified. (hereinafter, the Company) to public and private subjects (public administrations, professionals, etc.), and among these, also public and private health structures, for the booking of visits and diagnostic tests.

2. The preliminary investigation.

The verification activity, pursuant to art. 58 of the Regulation and 157 and 158 of the Code, involved both the Company (see inspection reports XX and XX, in the documents) and the Municipality of Rome, which uses the aforementioned application for the provision of services at the branch with respect to which the procedure was defined with provision dated 7 March 2019, n. 81 (web document n. 9121890).

The outcome of the investigations revealed that the "Tupassi" application is an interactive booking system with "eliminate queues" functionality that allows users to book counter services or make appointments, with public and private entities using various channels. The reservation can be made using the mobile app, the website (www.Tupassi.it and www.Tupassi.com), directly with the entity providing the service, through the use of totems positioned at the offices of the subjects who provide the services, or through subjects who provide users with the possibility of making a reservation through the system (so-called brokers, for example traders of revenue stamps and tobacconists).

In this context, through the "Tupassi" application, the Company collects users' personal data, both when registering the account (name, surname, tax code, mobile phone number and e-mail address and a second optional telephone number), and at the time of booking the appointment (chosen structure, date, time, type of service).

The system also allows you to book, modify or cancel appointments, not only by the interested party for his own needs, but also on behalf of third parties, whose data is entered into the system by the account holder who makes the reservation (name , surname, tax code, e-mail address and telephone number of the person for whom the appointment is being booked). A summary of the reservation, with the name, surname and tax code of the person to whom the booked service refers, is sent to the e-mail address associated with the user's account.

The application also allows the public and private entities that use it to also process data relating to internal staff who manage the various user requests (office workers, and other employees with different tasks and qualification profiles) and to extract a report containing data relating to the management of the various services provided.

The booking management software is supplied to the customer with a license for use: the Company usually guarantees the assistance and maintenance service as well. In this case, the software is installed on the customer's servers dedicated to the service and operates autonomously. The personal data collected during the account registration phase are stored on the Company's servers; the same data, together with the data relating to the service booked, are also stored on the client's servers (see report XX).

In particular:

- to use the service, via mobile app or website, users must register by creating an account, which allows you to book appointments with all the subjects who use "Tupassi" (report XX, cit.);
- in such cases "the systems of Miropass S.r.l. by querying the clients' servers, on which the aforementioned management system must be previously installed, provide the user with the list of available services, as decided by the client himself [or the entity that uses the booking system]; the user, therefore, by selecting the service and the date of the appointment, causes the system [managed by] Miropass to transmit the information to the customer's server and it is registered in the "Tupassi" booking management system used by the customer himself";
- these data flows take place via "HTTPS protocol, while those locally ("Tupassi" reservation management totem and vice versa) can, at the customer's choice, take place either in https or in http, the latter being chosen as the transmission of the data takes place within a LAN";
- with regard to "the use of the totem, it is the customer [i.e. the entity that uses the booking system], on the other hand, who defines whether and what information to acquire from the user for the booking; the latter data is recorded on the customer's servers and do not involve any creation of the Miropass S.r.l. account." (report XX, cit.);
- overall, the service offered includes the supply of the "Tupassi" booking management system, [...] to which Miropass S.r.l. can add the assistance and maintenance service";
- concretely "the assistance/maintenance intervention can take place either through direct access to the server through authentication credentials, provided by the customer, or through a graphical interface" (see report XX);
- access to customer servers for assistance/maintenance takes place via a VPN connection, upon authorization by the customer who generally provides a username and password via two different channels, i.e. the first via e-mail and the second via text message;

- as regards access credentials to customer servers, the Company has declared that it has received personal credentials;

- the Company forwarded "a PEC to all customers in which it raised awareness of the update to the latest version of the "Tupassi" booking management system, in line with the GDPR" (see report XX);

- "none of the customers has appointed [the Company] as data controller for the assistance and maintenance activity" nor as "system administrator of the customers' servers, to which they access directly, from the command line, for the activity of assistance/maintenance" (see report XX);

- the Company makes available on its website "privacy information and cookie policy", complete with the elements required by art. 13 of the Regulation;

- with regard to compliance with the obligations established by the personal data protection regulations, the Company declared that it had proceeded to designate the Data Protection Manager and to have carried out the impact assessment pursuant to art. 35 of the Regulation and has made available to the Authority the Register of treatments, compiled pursuant to art. 30 of the Regulation.

With a note of the XX (prot. n. XX), the Office, on the basis of the elements acquired from the checks carried out and the facts that emerged following the preliminary investigation activity, as well as the subsequent evaluations, 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 article 58, paragraph 2, of the Regulation, inviting the Company to produce defense 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 note mentioned above, the Office noted that the Company has implemented a treatment of the personal data of the interested parties, in the absence of:

- a suitable prerequisite for the lawfulness of the processing, both with regard to the data on the health of the data subjects who make reservations at health facilities through the "Tupassi" apps or websites, and with regard to the data (referring to users and employees of the entities that have adopted the system) processed during the performance of assistance and maintenance activities on behalf of the data controllers, in violation of art. 5, letter. a), 6 and 9 of the Regulation;

- identification of the retention period of the personal data of registered users (or the criteria for determining it), in violation of art. 5, par. 1, lit. e) of the Regulation.

- adequate regulation of the relationship with the cc.dd. brokers who carry out the treatments at the time of booking on behalf of the Company, in violation of art. 28 of the Regulation;

In relation to the aforesaid disputes, with note of the XX the Company sent its defense briefs, providing further elements during the hearing of the XX as well as transmitting documentation, with note of the XX prot. XX.

As regards the violation of the art. 9 of the Regulation, regarding reservations made at health facilities, made via app, website, or totem, the Company represented that: "the acquisition of the user's consent to the processing of health data, in the case of booking services at health facilities, the user is asked before entering the data.Exclusively for customers operating in the health sector, a function has been implemented which, for those who book on the website, automatically generates a pop up warning the user that this type of booking involves the processing of health data and prior consent to the processing is requested.For those using the mobile App, the user is prevented from continuing with the booking until after confirmation of reading the information and performance of the specific consent to the processing of this category of data" (report of the XX hearing).

With reference to the alleged violation of articles 5, letter. a), 6 and 9 of the Regulation, in relation to the processing of personal data in the absence of a suitable assumption of lawfulness, when carrying out assistance and maintenance activities on behalf of the data controllers, the Company represented that it had been designated responsible for data processing on behalf of the Roma Capitale il XX administration, specifying that the "maintenance and assistance activities (both of the server and of the Tu-Passi application) do not require or require access to the personal data of the user who has booked but only and exclusively in particular and occasional verification requests by the customer". With regard to the other entities to which the company has provided the application, the Company has represented that it has sent a communication stating that, in order to be able to carry out the assistance and maintenance activity which involves the processing of personal data by the Company, it is necessary to regulate the relationship pursuant to art. 28 of the Regulation, making himself available, alternatively, to carry out the assistance and maintenance activity without directly accessing the data, but providing the necessary support "exclusively, by email and/or telephone, ... on how to carry out, on your part, the verification" (defensive memoirs of the XX).

With reference to the violation of the art. 5, par. 1, lit. e), in relation to the failure to identify the retention times of data relating to users registered on the "Tupassi" system (or the criteria for determining them), the Company specified that "it had reduced the user's operating period from the previous 5 years one year, starting from the last use of the account by the user. As

regards the data relating to reservations, they are canceled after one month from the date of the appointment" (report of the XX hearing).

With reference to the violation of the art. 28 of the Regulation concerning the non-designation of "Tu-Passi booking agents". (so-called brokers, for example tobacconists), who make reservations for user services, through specific accounts, the Company specified that, although "in the time frame in which this service was active, the relationship with them pursuant to Article 28 of the GDPR", to date "considering the small number of bookings made through this channel, the broker accounts have all been disabled" (report of the XX hearing).

3. Investigation outcome.

Based on the regulations on the protection of personal data, the owner must process personal data (art. 4, n. 1, of the Regulation) in a lawful, correct and transparent manner (art. 5, paragraph 1, letter a) of the Regulation) and in compliance with the conditions set forth in art. 6 and 9 of the Regulation.

With regard to the particular categories of personal data, including those relating to health, in relation to which a general prohibition of treatment is envisaged, the same is permitted in the cases indicated in art. 9, par. 2 of the Regulation (see also art. 9, paragraph 4 of the Regulation and art. 2-septies of the Code).

Even in the presence of a specific assumption of lawfulness of the processing, the data controller is in any case required to respect the principles of "lawfulness, correctness and transparency", "limitation of purposes", "minimization", "limitation of conservation" as well as "integrity and confidentiality" of data and "accountability" (Article 5 of the Regulation).

3.1. Processing of users' personal data through the "Tupassi" platform for the purpose of registering and using the services.

In the light of the elements acquired and the declarations made during the preliminary investigation, the processing of personal data of users, during registration (creation of the account), as well as following the booking made, takes place within the scope of the provision of the service of booking appointments provided by the Company to client entities (see on this point, disclosure in documents) and is necessary for the execution of a contract of which the interested party is a party (Article 6, par. letter b) of the Regulation) .

With regard to the personal data relating to the booking of appointments, the system stores - also for the purpose of sending the interested party a summary of the booking on the app or by e-mail (see attachments to the minutes of the XX) - the data relating to the reservation associated with the account and in particular: the name, the user's tax code, the date, the time as

well as the structure/public body or private entity where the appointment is scheduled. In cases in which the booking concerns appointments with public or private individuals who provide healthcare services, the information on the aforementioned bookings can also be traced back to the particular categories of data governed by art. 9 of the Regulation, including those relating to the "provision of health care services" (art. 4, paragraph 1, no. 15 of the Regulation). Moreover, from the documentation acquired during the inspections, in some cases, the reservation at the selected healthcare facility also specifies the type of service chosen (e.g. blood sampling, exam collection, physiotherapy, dentistry, etc.).

Based on the regulatory framework in force, the processing of these categories of data can only take place when one of the cases referred to in art. 9, paragraph 2, of the Regulation which did not exist, at the time of the assessment, in the case in question.

Having acknowledged the measures adopted by the Company during the preliminary investigation in order to acquire the user's prior consent for the processing of the aforementioned type of data, it is, however, ascertained that the processing of personal data, associated with the booking of appointments for services health checks, carried out prior to the implementation of the aforementioned measures, were carried out in the absence of a specific consent of the interested parties, in violation of art. 9, par. 2, lit. a) of the Regulation.

3.2. Processing of personal data in the context of maintenance and technical assistance.

The legislation on the protection of personal data identifies the subjects - owner and manager - who, for various reasons, can process the personal data of the interested parties, also establishing their relative attributions.

In particular, the owner is the subject responsible for the decisions regarding the purposes and methods of processing the personal data of the interested parties as well as a "general responsibility" (accountability) on the treatments carried out by the same owner or by others who carry out such treatments "on your behalf", i.e. the data processors (cons. 81, articles 4, point 8) and 28 of the Regulation).

The relationship between the owner and the manager is regulated by a contract, or by another legal act stipulated in writing through which the owner gives instructions to the manager and provides, in detail, what the disciplined matter is, the duration, the nature and the purposes of the treatment, the type of personal data and the categories of interested parties, the obligations and rights of the owner. The data controller is therefore required to process the data of the interested parties "only on documented instructions from the owner" (Article 28, paragraph 3, letter a) of the Regulation).

With regard to the treatments carried out through the "Tupassi" platform, the Company processes the personal data of individual users registered on the platform by creating an account (see, disclosure in the documents), as part of the offer of the booking service through " mobile app or website", as owner.

Otherwise, the processing of personal data relating to bookings of appointments for the services provided at the counter made by users of the individual entities that use the "Tupassi" platform fall within the ownership of the individual entities. In fact, they pursue their own goals, in terms of efficiency and productivity (whether they are public or private subjects) for the execution of tasks in the public interest or in the context of the exercise of the business activity.

With regard to the assistance and maintenance activity carried out by the Company on the booking management system installed on the customers' systems - an activity which, when it does not exclusively concern the hardware component of the systems, but includes, as in the present case, the possibility that the staff authorized by the Company to access the management of customers, inevitably also involves the processing of personal data of users -, the failure to adopt suitable acts to identify the same as data controller (see Article 28 of the Regulation) is not compliant with the discipline of data protection.

Otherwise, this regulation is not due in cases in which the company carries out technical assistance exclusively through mere support (telephone or email), without direct access to the systems and the personal data contained therein.

This circumstance, ascertained during the checks carried out at Roma Capitale (see provision no. 81 of 7 March 2019, see par.3.3.), was confirmed by the Company also with regard to the other entities that use the assistance and maintenance service and has resulted in the fact that, limited to assistance and maintenance operations, the Company has processed personal data, referring both to users and to employees of the entities that have adopted the "Tupassi" platform, in the absence of a suitable legal basis, in violation of the articles 5, par. 1, lit. a), 6 and 9 of the Regulation.

3.3. The treatments carried out by the Booking Agents.

Based on the investigation carried out, the booking of appointments with the "Tupassi" system could also be made by users through intermediaries ("Tupassi" booking agents, so-called brokers).

With respect to the aforementioned intermediaries, the Company has declared that it has failed to regulate the related relationship, in violation of the provisions of art. 28 of the Regulation.

This booking channel, which had involved a small number of intermediaries with a limited response in terms of bookings from users, was deactivated by the Company in 2019, during the investigation.

3.4. Definition of retention times for personal data.

In the light of the investigations carried out, it emerged that "[...] the accounts are deactivated automatically after 60 months of inactivity or by the operator's hand" and also, in the event that the user cancels his account, "the deleting the account involves removing the tax code and telephone numbers from the database as well as the list of all the subjects for whom appointments have been booked, leaving only a trace in the "m_account_aud" table of the name, surname, email address and consents privacy, together with the date and time of the individual operations, for any responses to future disputes".

Although during the hearing before the Guarantor the Company specified that "it had reduced the period of operation of the user from the previous 5 years to one year, starting from the last use of the account by the user" and that the information relating to reservations "are canceled after one month from the date of the appointment", it is in any case ascertained that previously, both in the case in which the account was deactivated due to inactivity, and in the case in which the user proceeded to cancel his account, users' personal data were kept for an indefinite time by the Company, in violation of art. 5, par. 1, lit. e) of the Regulation.

Moreover, from checks carried out by the Office it has also emerged that the text of the information made available online to users has not yet been updated with regard to the retention times represented by the Company during the preliminary investigation.

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 and during the hearing before the Guarantor of the truthfulness of which one may be called 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.

In order to determine the applicable rule, in terms of time, the principle of legality pursuant to art. 1, paragraph 2, of the law no. 689/1981 which provides that «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 offenses - must be identified at the time of cessation of the unlawful conduct, which occurred after the date of 25 /5/2018 in which the Regulation became

applicable.

The preliminary assessments of the Office are therefore confirmed and the illegality of the processing of personal data carried out by the Company is noted, in violation of the basic principles of the processing, in the absence of an appropriate legal basis for the processing of personal data of users and employees of the entities to which the "Tupassi" platform has been provided, and without having regulated the relationship with the so-called "Booking agents", cc.dd. broker, in violation of articles 5, par. 1, lit. a) and e), 6, 9 and 28 of the Regulation.

The violation of the aforesaid provisions renders the administrative sanction foreseen by art. 83, par. 5 of the Regulation, as also referred to by art. 166, paragraph 2, of the Code.

In this context, considering that the conduct has exhausted its effects, given that the relationship with Rome has been regulated pursuant to art. 28 of the Regulation, that the Company has made improvements to the "Tupassi" system, providing for the need for consent for the purpose of booking services at health facilities, defining limited retention times for the data of account holder users, in relation to the termination of the use and arranging the deactivation of the booking channel through Booking Agents, cd. broker, the conditions for the adoption of corrective measures pursuant to art. 58, par. 2, of the Regulation, in relation to the disputed critical issues.

However, it should be noted that following the identification of retention times for account holder user data, the text of the information made available online needs to be updated in relation to the aforementioned time period as defined by the company during the preliminary investigation.

5. Adoption of the injunction order for the application of the pecuniary administrative sanction and accessory sanctions (articles 58, paragraph 2, letters i and 83 of the Regulation; article 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, depending on the circumstances of each single case" and, in this framework, "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, taking into account the art. 83, par. 3 of the Regulation, in this case - also considering the reference contained in

art. 166, paragraph 2, of the Code – the violation of the aforementioned provisions is subject to the application of the same pecuniary administrative sanction provided for by art. 83, par. 5, 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 particular delicacy of the data of users who make use of the appointment booking service relating to health services was considered (Article 4, paragraph 1, no. 15 of the Regulation) and the large number of interested parties , including those relating to users and employees of the entities to which the Company has provided the "Tupassi" platform, treated by the Company in the activity of assistance and maintenance on the systems.

On the other hand, it was favorably noted that the Company has taken steps to bring processing into line with the regulations on the protection of personal data (regulation of the relationship pursuant to Article 28 of the Regulation, acquisition of consent for the processing of data pursuant to Article 9 of the Regulation, identification of data retention times), collaborated with the Authority during the investigation of this proceeding. There are no previous relevant violations committed by the data controller or previous provisions pursuant to art. 58 of the Regulation.

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction also taking into account the phase of first application of the sanctioning provisions pursuant to art. 22, paragraph 13, of Legislative Decree lgs. 10/08/2018, no. 101, to the extent of 40,000.00 (forty thousand) euros for the violation of articles 5, par. 1, lit. a) and e) as well as articles 6 and 9 and 28 of the Regulation.

Taking into account the particular delicacy and the number of data processed, it is also believed that the accessory sanction of publication on the Guarantor's website of this provision should be applied, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Regulation of the Guarantor n. 1/2019.

Finally, it should be noted that the conditions pursuant to art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

6. Corrective Measures.

While acknowledging what emerged from the defense briefs and while taking into account the measures already introduced, which have been acknowledged in paragraph 5, it is necessary to enjoin the Company, pursuant to art. 58, par. 2, lit. d), within and no later than thirty days from the date of receipt of this provision, to integrate and update the text of the information made

available online with all the elements referred to in articles 13 and 14 of the Regulation with particular reference to the retention times as defined by the company during the preliminary investigation.

ALL THIS CONSIDERING THE GUARANTOR

detects the illegality of the treatment carried out by Miropass S.r.l., for violation of the articles of the articles 5, par. 1, lit. a) and e) as well as articles 6 and 9, as well as 28 of the Regulation in the terms referred to in the justification;

ORDER

To the company Miropass S.r.l. in the person of the pro-tempore legal representative, with registered office in Via Rivafredda, n. 3, Crema, P.I. 07826360963, to pay the sum of 40,000.00 (forty thousand) euros as an administrative fine for the violations indicated 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 the same Company to pay the sum of 40,000.00 (forty thousand) euros, 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 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) pursuant to art. 58, par. 1, lit. a), of the Regulation, and of the art. 157 of the Code, the company - data controller - to communicate, by providing adequately documented feedback, within and no later than thirty days from the date of receipt of this provision, the initiatives undertaken in relation to the provisions of point 6 above). Failure to respond to a request pursuant to 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

pursuant to art. 166, paragraph 7, of the Code, the publication of this provision on the Guarantor's website, believing that the conditions set out in art. 17 of the Regulation of the Guarantor n. 1/2019.

Pursuant to art. 78 of the GDPR, of the articles 152 of the Code and 10 of Legislative Decree 1 September 2011, n. 150, 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, 17 December 2020

PRESIDENT

Station

THE SPEAKER

Station

THE SECRETARY GENERAL

Matthew