[doc. web no. 9831081]

Injunction order against the ODV Covid-Healer Association - 20 October 2022

Register of measures

no. 336 of 20 October 2022

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 dr. Claudio Filippi, deputy secretary general;

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 the Code regarding the protection of personal data (legislative decree 30 June 2003, n. 196), as amended by legislative decree 10 August 2018, n. 101, containing provisions for the adaptation of the national legal system to the aforementioned 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 4/4/2019, 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 office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web no. 1098801;

Speaker the lawyer Guido Scorza;

WHEREAS

1. Introduction: the Covid Healer application

This Authority has become aware, through elements found at the following link, https://www.insicurezzadigitale.com/covid19-cure-domiciliari-e-app-sospette- ATTENTION/, that the Covid-Healer Association

- ODV (of hereinafter the "Association") has created the Application called "Covid Healer" (hereinafter also only the "App"), qualifying itself as the owner of the processing of personal data of users and health professionals who use it, as well as the subject to whom you are entitled to all rights relating to the same (see "Terms of use and privacy policy" available at https://covidhealer.org/termini-duso-e-privacy-policy/).

More precisely, the aforesaid document containing "Terms of use and privacy policy" highlights that the Association, as data controller, in relation to the "Patient User" (the subject, natural person who through the App requests consultancy and/or health assistance for the treatment of the pathology from which he is affected), processes "the data that the User spontaneously provides during registration and account creation or even subsequently such as, by way of example, name and surname , date of birth, telephone number, residential address, e-mail address or others" as well as "the data relating to one's health that the User spontaneously provides during registration and account creation or even subsequently such as, by way of example, blood pressure, blood sugar, allergies, intolerances, the presence of particular pathologies or the intake of certain drugs or others".

Furthermore, in the same document, it is specified that the Association, as owner, also processes the personal data of the Healthcare Professional User, i.e. "the natural person who, through the App, on a non-profit basis and therefore for purposes other than and unrelated to his professional activity, provides the patient with advice and/or health care for the treatment of the pathology from which the latter is affected".

2. The preliminary investigation

With a note of the XX, the Association responded to the request for information from the Office (note of the XX, prot. n. XX), regarding the aspects of protection of personal data concerning users (both patients and health professionals) who use the C-Healer App.

In particular, the Association represented that:

- the C-Healer App aims "to facilitate contact between the patient and medical personnel" who (...) "have decided to collaborate with the same [Association] and provide voluntary and free assistance to the User-Patients who needed", taking into account "the effects that the Covid-19 pandemic has had not only on the population, but also on accessibility to health services and facilities";

- "Once the Healthcare Professional has been identified and a connection between this and the User-Patient has therefore been guaranteed, the Association leaves the Healthcare Professional (already independent Data Controller in the GDPR area)

with the exclusive responsibility and the necessary autonomy to provide Users-Patients with the interventions and social-health services deemed appropriate";

- "the data processed through the use of the C-Healer Application relate to interested parties that qualify as Users-Patients and Users-Healthcare Professionals-Doctors";

- the Healthcare Professional-Medical "operates, in relation to the care and monitoring activities of Patients-Users, as an Independent Data Controller, assuming obligations and responsibilities related to the role held; the Agreement drawn up by the Association which identifies the independent Healthcare Professional is currently being formalised";

- the Association "assumes the role of Independent Controller exclusively for the purposes of mere organization of activities aimed at solving health problems due to the SARSCoV-2 Coronavirus and for the related fundraising activities, as well as facilitating communication between the User-Patient concerned and the User-Healthcare Professional (formerly independent Data Controller pursuant to the GDPR)";

- "the purposes of the processing pursued through the use of the App and relating to users can be summarized as follows:

a) allow registration to the Application and, therefore, allow the functioning of the same and access to the services offered through this tool;

b) carry out the maintenance and technical assistance necessary to ensure the correct functioning of the App and the services connected to it, including any implementation also for any new features;

c) respond to the requests of the User and to those who have spontaneously sent their personal data;

d) fulfill the obligations established by current laws, regulations or community legislation, or satisfy requests from the Authorities;

e) collect information, in aggregate form, on the number of users and how they use the App;

f) allow the Owner to exercise their rights in each location and repress any unlawful behavior connected with the use of the App or the services offered through it";

- the legal bases of the processing have been identified, among others:

"for the processing of non-particular data, in the execution of a contract and pre-contractual measures, without economic consideration, referred to in letter b), of par. 1, of the art. 6 of the GDPR;

for the treatment, however, of particular data (including their transfer to doctors adhering to the App), in the consent given by

the interested party, pursuant to letter a), of par. 2, of the art. 9 of the GDPR";

With specific reference to the acquisition of the consent of patient Users, the Association has declared that:

"The operating system developed through the App allows you to keep track of the release of consent in relation to the purposes indicated in the information document made available by the Data Controller" and "of the moment in which this consent is released";

"when the User proceeds with the application to join the App by starting the procedure for creating a new Account, the system requires, in addition to entering some initial personal data (i.e.: name, surname, email address and a personal password), acknowledgment and simultaneous acceptance of the terms of use of the Application and acknowledgment and acceptance of the privacy policy";

after confirmation of the email address through the specific link sent to the User, the latter "will be able to access the next phase of registration, entering the additional requested data (such as, by way of example: User's image, date of birth , gender, address) and attaching the documentation useful to allow the Association to carry out the necessary checks on the identity of the User", which would be kept in the manner described, in the aforementioned acknowledgment note of the XX;

to follow, "the registration request is taken over by the Association, through specifically identified subjects (appointed "Authorised" for processing), who will proceed with the approval of the registration if all the required conditions are met";

"the system will send an alert to the e-mail address indicated by the interested party with which the User is asked to send, by e-mail to the addressregistration@covidhealer.org, a copy of the form relating to the issue of consent (findable at the following link Consenso_informato-1 .pdf (covidhealer.org)), duly completed in all its parts and signed by the interested party".

The Association has also highlighted that the need to acquire the identity document of the person who intends to register with the App derives in particular not only from security needs, but also to prevent subjects who do not really intend to use the services offered from registering, or "prevent the registration to the Application by subjects other than those who will then go to ask for and obtain medical assistance from Health Professionals (...) whose conservation, however, will be temporally limited only to control and verification activities of the actual existence of the Patient and, in any case, will not exceed the day of the verification".

In relation to the fulfillment of the information obligations, pursuant to articles 13 and 14 of the Regulation, the Association represented that the information is provided to interested parties upon registration to the App.

The Association also briefly illustrated the security measures implemented. In particular, the data would be stored in the Cloud using only the services made available by Google, in the EU or in the EEA, which do not involve transfers, storage or processing of data outside the aforementioned territory.

As regards the performance of the impact assessment pursuant to and for the purposes of art. 35 of the Regulations, the Association declared that:

- "the activities aimed at its preparation are underway even if at the moment the existence of high or elevated risks for the rights and freedoms of the interested parties has not been detected, also in consideration of the security measures implemented";
- “In this regard, it is deemed appropriate to recall what, moreover, reported in this regard by the Guidelines WP 248 rev. 01 of the WP29 which reiterate that in the absence of high risks for the freedoms and rights of the interested parties, the Data Controller may decide not to carry out the Impact Assessment (see page 13)";
- "to date, not even the "large scale" requirement can be considered configured, at least with reference to particular data which, on the basis of the number of User-Patients currently assigned to be treated by Healthcare Professionals, does not appear to be more than 500 units" .

Finally, the Association produced a Register of processing activities dated 17 January 2022, subsequently amended and attached to the note of the XX.

On the basis of the elements acquired in the context of the preliminary investigation, the Office, with an act of the XX (prot. n. XX), notified on the same date by certified e-mail, which must be understood as reproduced in full here, initiated, pursuant to of the art. 166, paragraph 5, of the Code, with reference to the specific situations of illegality referred to therein, a procedure for the adoption of the provisions pursuant to art. 58, par. 2 of the Regulation, against the Association inviting it 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, law n. 689 of 24 November 1981).

With the aforementioned deed, the Office found that the Association had processed health data in the absence of a suitable legal basis in violation of articles 5, par. 1 lit. a), 6, 7 and 9 of the Regulation. Furthermore, taking into account the aforementioned ownership of the treatment of the Association and of the health professionals and since no designation as responsible for the treatment has been made, pursuant to art. 28 of the Regulation, the Office has ascertained that the

Association has communicated data on the health of patients to the aforementioned professionals in the absence of a suitable legal prerequisite and therefore in violation of articles 5, par. 1 lit. a) and 9 of the Regulation. The office.

With specific reference to the disclosure model provided by the Association, the Office has ascertained that it violates the principles of correctness and transparency of data (articles 5, paragraph 1, letter a), 12 and 13, of the Regulation). Lastly, the Office found the violation of the art. 30 of the Regulation, as the register of treatments produced in deeds was found to lack some of the minimum information that it must contain pursuant to the aforementioned art. 30, par. 1 of the Regulation and also drawn up after the treatment has begun. Furthermore, the violation of art. 35 of the Regulation taking into account that, on the basis of the elements acquired following the preliminary investigation, as well as the subsequent assessments carried out, it has been ascertained that the case in question is one of those for which the controller is required to carry out, "before proceeding to the treatment, an assessment of the impact of the envisaged treatments on the protection of personal data".

3. The defense briefs

With note of the XX, the C-Healer Association sent its defense briefs, also asking to be heard, pursuant to art. 166, paragraph 5 of the Code, in which it was generally represented that:

"the intention of the Association has always been to pursue its mission of support and assistance to those affected by the consequences of the pandemic crisis in the context of an objective emergency situation, respecting the regulations";

"to prove the seriousness of the project (...) the initiation of the preliminary phase of this preliminary investigation has led the Association to block any operation of the App, simultaneously launching a gradual and progressive process of adaptation and improvement";

With specific reference to the objections raised by the Office in the deed of initiation of the sanctioning procedure pursuant to art. 166 paragraph 5 of the Code, the Association highlighted the following.

3.1 On the identification of privacy roles

In relation to this profile, the Association has declared that:

"after having managed the User-Patient registration phase in the Application and having guaranteed the correct registration of the same and the creation of his/her User profile, he leaves the Healthcare Professional with the exclusive responsibility and the necessary autonomy aimed at providing the User-Patients the interventions and social-health services deemed appropriate to fulfill the mission pursued";

"there is no doubt about the qualification of the same as Independent Data Controller: each Doctor, in fact, in relation to the care and monitoring activities provided to the Patient-Users, assumes obligations and responsibilities related to the role covered, with the consequences which derive from this not only in terms of medical liability (a topic which it is not deemed necessary to go into further detail here) but also in relation to the treatment of the health data of the same Users-Patients";

"the individual Doctor will provide the User - when he comes into contact with the Patient entrusted to him for the first time - his own information pursuant to art. 13 GDPR with which it will make these subjects informed about the methods and purposes of treatment pursued by the same. C-Healer will inform the User-Patients of this fulfillment already within its information pursuant to art. 13, adequately reviewed and implemented during the adaptation process initiated by the Data Controller pending this proceeding (please refer to the content of the specific information notice pursuant to article 13 in the updated version made available therein by this esteemed Authority and which will be explained more fully hereinafter - see Doc. 2 - Disclosure pursuant to art. 13 Patient Users (updated))";

"In fact, in the aforementioned disclosure (...) we read how the Healthcare Professional, once the assignment of the Patient has taken place, becomes and operates as an Independent Data Controller";

"the same Agreement that the Doctors sign with the Association (...) reaffirms the duty of each Professional to take charge of promptly identifying the purposes, methods and means of processing the personal data of the patients that will be assigned to them"

“(…) there is no doubt that the role of this technological tool developed by C-Healer can only be that of a mere contact tool between the two types of Users of the same: Patients, on the one hand, and Doctors, on the 'other";

"once the individual Patient has been assigned to the Doctor, the latter as a healthcare professional, a subject with the legal requirements to carry out the activity of care assistance, assumes the status of Independent Data Controller in relation to the personal data processed for these purposes , at the same time appointing the Association in charge of the treatment pursuant to art. 28 GDPR, limited to the provision of the platform as a tool used by the Doctor to carry out the treatment and assistance activity with greater timeliness and efficiency";

"The Association, in fact, in this second "segment", acting as a mere data processor, will limit itself to acting as a "database" of the information collected and to provide the service of "management and use of the application created to allow of patients/users" and according to the timing set out in the agreement with the Doctor, will proceed with the cancellation of all

information, even sensitive and particular, relating to individual Patients".

3.2 On the legal bases of the treatment

The Association reiterated that:

"as regards the (...) purposes related to the registration to the Application and the possibility of allowing the functioning of the same, as well as access to the services offered through this tool (...), the legal bases have been identified (...):

- for the processing of non-particular data, in the execution of a contract and pre-contractual measures, without economic consideration, referred to in letter b), of par. 1, of the art. 6 of the GDPR;

- for the treatment, however, of particular data (including their transfer to the Doctors adhering to the App),

in the consent given by the interested party, pursuant to letter a), of par. 2, of the art. 9 of the GDPR";

"the information originally prepared by the Association and made available in a preliminary phase directly on the App underwent a process of improvement and modification during the adjustment activity started, in the meantime, by C-Healer. As a result of these changes, the Association has thus prepared a new information pursuant to art. 13 GDPR aimed at Users-Patients who are about to request registration and the simultaneous creation of a profile through their App";

"From reading this document in its updated version - which we would like to point out is not yet available to interested parties, due to the current status of blocking/suspension of the Application - it emerges peacefully that individual Users-Patients will be able, in extremely clear manner, know the purposes and legal bases underlying the individual treatments put in place by Covid-Healer, as Data Controller and, at the same time, become aware of the possibility that the Association transfers their personal data to subjects third parties (read Healthcare Professionals) only and exclusively following the release of their consent, so that the latter can - in turn as Independent Data Controllers - carry out those specific processing activities connected to the required care and assistance services ";

"in the new version of the disclosure pursuant to Article 13 of the GDPR released to User-Patients, the latter will be made aware of the fact that each Doctor, once he has taken charge of the single position of the User entrusted to him, will undertake to provide each of them "the appropriate information pursuant to art. 13 of the GDPR, also in relation to storage times, as well as taking over from Covid Healer - ODV, also for the management of User requests and communications".

In relation to consent as a valid legal basis for the processing of personal data of patient users, the Association represented that:

“There is no doubt, (…), on the legitimacy of this legal basis deemed viable by the GDPR itself which, in art. 9, par. 2, lit. a) identifies precisely in the "consent of the interested parties" one of the legitimizing reasons for the processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or union membership, as well as processing genetic data, biometric data intended to uniquely identify a natural person, data relating to a person's health or sex life or sexual orientation”; and the "correct implementation of a consent collection system that complies with regulatory requirements";

"Precisely to guarantee this last requirement, the Association has improved and implemented its processes for collecting the consents of the interested parties, going so far as to separate, in a timely manner, the moment in which the User-Patient gives his consent to the loading of his personal data to the App from the one in which the same User grants his authorization to transmit such data to a third party (the Health Professional), so that the latter can provide his own support and his own care and assistance services (yes refer for further details relating to the methods of obtaining consent implemented by the Association during the adaptation process initiated by the same (...)";

"The Association keeps evidence of these elements through a procedure for tracing the logs connected to the activities and/or accesses made to the App through the services offered by its Cloud service provider";

"The Association - as part of the process of gradual adaptation and improvement of its privacy structure - is evaluating the implementation of a system that will allow it to also keep track of the successful release of consent by the Interested Users. The system, therefore, would be implemented with a mechanism capable of allowing the automatic sending to the Patient of an email with the confirmation of the registration and of the consents issued";

"the Association has developed a new system for the collection and management of privacy consents relating to the processing of personal data of Users-Patients";

"After this preliminary phase, the system will generate two new requests for consent, connected to the purposes referred to in the information pursuant to art. 13 of the GDPR. More specifically, the App will ask the User-Patient to provide their consent in relation to:

Uploading information on the health status and clinical picture of the user-patient on the C-Healer App, in pseudonymized mode, following the request for assistance by the interested party and, more generally, facilitating the dialogue between the same (Requesting Patient User) and the Healthcare Professional User - Accepting Physician, until the relative combination of

these two subjects;

- Communication of personal data of Patient Users, including those relating to health, to Healthcare Professional Users registered on the App, so that they can give their support and services, involving the related archiving (such Professional Users, as mentioned above, from receipt onwards or in any case from the combination, will process the data as independent data controllers);

The consents, possibly issued, by the User-Patient with reference to these two specific purposes of treatment - and of which the Association will keep track in compliance with the above in greater detail - will allow the Association to operate in respect and in accordance with the purposes prosecute";

"In the event that, (...) a User-Patient decides not to give his consent in relation to one or both of the above purposes, the use of the Application will remain limited to mere registration and/or the sole purpose for to which consent has been given. This is due to the fact that without the specific consents, the Association will respectively be unable to upload the particular personal data of the User-Patient to the App nor, a fortiori, transfer them to a third party such as the Healthcare Professional";

"As regards (...) the processing of personal data of Users-Healthcare Professionals, the Association, precisely in order to make its position more intelligible and transparent towards all interested parties, has separated this information by creating a document ad hoc information which, in compliance with the provisions of art. 13 of the GDPR, allows in a simple and clear way to identify the different types, purposes and related legal bases relating to the processing of personal data of Healthcare Professionals;

"each User-Patient will have the opportunity to exercise his right of revocation in relation to the consents granted (in compliance with the express provisions of articles 6, paragraphs 3 and 4) by contacting the Association at the addresses indicated in the Information itself (including, it will be noted, there is also the contact address of the Personal Data Protection Officer, adequately identified and appointed in the meantime)".

3.3. On information to data subjects and on the rights of data subjects

In relation to the information to be provided to interested parties, the Association clarified that "the two types of interested parties-Users (Patients, on the one hand and Healthcare Professionals, on the other) will receive, from the moment in which operations are restarted of the App, the new version of the information, specifically dedicated to them, pursuant to and by effect of art. 13 of the GDPR. The need to further differentiate the information made available to Users became evident in the

broader process of adapting the privacy system launched by the Association during the initial phase of the current preliminary procedure. With reference to the ways in which the references to the rights exercisable by the interested parties were expressed in relation to the treatments put in place by the Association, the latter highlighted "like what is contained within the information disclosed to the Users (and contested by this Authority) literally reported the content of the GDPR rules. This also happened with regard to profiling (...) except, then, in the detail part (...), clearly clarifying how these alleged marketing and profiling activities, in reality, are not in any way carried out by the latter. For the sake of clarity and transparency, however, in the new updated versions of the two information notices, the Association has completely eliminated this reference".

With regard to the exact indication of the retention times of personal data in relation to the specific processing purposes, the Association clarified that "in the new information, (...) for each individual processing purpose, in addition to the precise indication of the legal basis foundation, a detailed and more specific retention period for the personal data processed is identified, indicating one or more retention terms of the same in relation to the specific treatments connected to the individual purposes under discussion".

3.4 On the Impact Assessment

In this regard, the Association confirmed that "in the context of the already mentioned several times above, process of adaptation to the privacy legislation initiated by the Association pending the present preliminary/sanctioning procedure (the same) is completing the activities connected to the preparation of this document", despite not having "detected the existence of high or high risks for the rights and freedoms of the Users-interested" and deeming, due to the security measures implemented "more than adequate the level of security achieved and low the risk connected to the treatments carried out, which in any case does not involve a number of users falling within the context of the "large scale".

3.5 On the register of processing activities

In this regard, the Association clarified that "in the second of the three worksheets (called: "Register of Treatments") from which the document is composed, all the elements allegedly considered absent are present: - categories of data recipients (art. 30, paragraph 1, letter d), see columns U, V and W); - purposes pursued (Article 30, paragraph 1, letter a), see column A); - legal bases of the treatment, see column Q; - data retention terms (art. 30, paragraph 1, letter f), see column X)".

This document was then updated "as part of the overall implementation and adjustment plan launched pending the present preliminary/sanctioning procedure" attached to the defense briefs.

4. The hearing held at the Guarantor

On the 20th date, the hearing was held during which the Association - while reserving the right to produce further documentation - in addition to what is already in the records, declared that:

"Following the preliminary intervention of the Guarantor, the application was suspended having [the Association] the intention of resuming its use only when it will be fully compliant with the regulation of the protection of personal data, a fundamental interest of the Association and which probably in the initial phase of development of the app it was not the object of sufficient attention by the lawyers involved at the time by the Association itself. It should also be noted that the app has been active for just over a month, involving around 20 doctors";

"the project is not for profit and that (...) has an interest in improving the same also from the point of view of the protection of personal data and that for this purpose has entrusted the care of privacy aspects to other lawyers, which demonstrates of [one's] good faith";

"access to the application is free and the intervention of doctors is carried out pro bono";

"no reports or complaints have been received regarding the processing of data carried out through the app".

Finally, the Association in expressing "its maximum cooperation" requested the filing of the administrative procedure and, subordinately, "even without acknowledging the validity of the objections, the application of a sanction in the smallest amount possible considering that the Association is a non-profit organization which is supported by liberal donations".

5. The supplementary documentation produced

With a note of the XX, the Association produced supplementary documentation in particular reiterating that it had "started a progressive process of adapting its structure and its Privacy Management System to current legislation, also in relation to the specific needs that emerged from the first, short, period of operation of the App (it should be remembered, approximately a month and a half, from 24 December 2021 to 5 February 2022, when the functionality and operation of the App were interrupted)". This led to a further integration and revision activity of the documentation already produced in deeds.

In this regard, the Association has transmitted the "Covid-Healer Agreement Template - Doctor/Healthcare Professional" in which "the obligations and responsibilities of the individual Doctor are precisely defined in relation to the processing of personal data carried out and with reference to the use of the App developed by Covid-Healer" and "the role in terms of privacy of each of them. In particular, "the Association assumes the role of Independent Data Controller" exclusively for the purposes of

promoting the service, organizing and promoting activities aimed at solving health problems due to the SARS-CoV-2 coronavirus and the related collection activities funds, as well as facilitating collaboration and dialogue between the requesting interested party and the accepting doctor, also by means of the collection of registration requests from users", while, as regards the "management and use of the application created to allow the treatment of patients-/users by Doctors", the same Covid-Healer will receive the appointment as external manager of the treatments (pursuant to and for the purposes of art. 28 GDPR). "The individual Doctor/Healthcare Professional assumes the role of Independent Data Controller as far as connected to all treatments aimed at" the management of requests for assistance from the user-patient through the appropriate indications and the necessary support, including, also, the activities of archiving and modification of the data of the interested parties".

In relation to privacy roles, the Association has also produced the "Appointment of Covid-Healer as External Data Processor pursuant to art. 28 of the GDPR".

The actions taken by the Association have also led to further changes to the privacy information to be made to Users - Patients at the time of creating the account on the App and to the treatment register, the updated copies of which have been acquired in the proceedings. Lastly, the Association represented that "to facilitate and facilitate the activity of individual Healthcare Professionals, it has undertaken to provide [them] with the necessary support for the preparation of a draft Information pursuant to art. 14 of the GDPR that the Doctors themselves will have to adapt and return to the patients once the matching and taking charge of them has taken place. [Notwithstanding], in any case, the right of each individual Healthcare Professional not to accept the draft Information made available by Covid-Healer and choose to use one prepared and personally adapted by them".

6. The outcome of the preliminary investigation: the violations ascertained

The preliminary investigation activity and the proceeding initiated by the Office, pursuant to art. 166, paragraph 5, of the Code, concerned the processing of personal data carried out by the Association through the C-Healer mobile application, which aims to put Patient Users and Healthcare Professional Users in contact - to allow Patients who show the symptoms of Covid-19 to be able to request remote assistance from a Healthcare Professional User.

In this regard, having taken note of what is represented by the Association in the documentation in the deeds and in the defense briefs, the following is observed in relation to the aforementioned treatments.

6.1. The principle of lawfulness of the processing of personal data (Article 5, paragraph 1, letter a), 6, 7 and 9 of the Regulation)

In the first instance, the Office contested the violation of art. 5, par. 1, lit. a) of the Regulation, which provides for compliance with the principle of lawfulness, according to which any processing of personal data must be based on a specific legal basis. In the event that the condition of lawfulness is represented by consent, it must be provided through a positive deed with which the interested party expresses a free, specific, informed and unequivocal will relating to the processing of personal data concerning him. If the processing is aimed at pursuing multiple purposes, consent must be given for each of these purposes (Recital 32, 42 and 43, articles 5, 6, paragraph 1, letter a) and 7 of the Regulation and Guidelines 5/2020 on consent pursuant to Regulation (EU) 2016/679, adopted by the European Committee for the protection of personal data, on 4 May 2020; sent. C-673/17, of 1 October 2019 and C-61/19, of 11 November 2020).

With specific reference to the particular categories of data, which include health data, the art. 9 of the Regulation establishes a general prohibition on the processing of such data unless one of the specific exemptions to this prohibition applies, among which the consent of the interested party is required. This consent, taking into account the nature of such data, particularly sensitive in terms of fundamental rights and freedoms, must also be explicit (Article 9, paragraph 2 letter a) of the Regulation and par. 4 of the Guidelines 5/2020 on consent pursuant to Regulation (EU) 2016/679, adopted by the European Data Protection Committee on 4 May 2020).

The regulation on the protection of personal data also provides - in the health sector - that information on the state of health can only be communicated to the interested party and can be communicated to third parties only on the basis of a suitable legal prerequisite or on the indication of the interested party same subject to written authorization from the latter (Article 9 of the Regulation and Article 83 of Legislative Decree No. 196 of 30 June 2003 (Code regarding the protection of personal data - hereinafter, the "Code").

In the case in point, the documentation in the proceedings has ascertained the violation of the principle of lawfulness of the treatment, since at the time of the facts the Association, in relation to patient data, for certain treatments (indicated in point 2 of the information prior to changes made during the procedure) it qualified as data controller (art. 24 of the Regulation). In relation to the medical and health services rendered by health professionals, the data controller has been identified in the health professionals themselves (see note replying to the Authority's request for information, of the XX). Taking into account the

aforementioned alleged ownership of the treatment of the Association and of the health professionals and since no designation of data controller has been made among these subjects, pursuant to art. 28 of the Regulation, it is ascertained that both the collection of patient data by the Association and the subsequent communication of such data on health to the aforementioned professionals took place in the absence of a suitable legal prerequisite and therefore in violation of articles 5, par. 1 lit. a) and 9 of the Regulation.

In this regard, in fact, the consent given by the patients, to which the Association refers in the documentation in the documents, cannot be considered a valid legal basis, neither for the collection, nor for the communication of such data. This is because this consent is not indicated in the section relating to the legal bases of the processing of the privacy information given to the interested parties, in the version prior to the changes made during the procedure.

From the documentation in the documents it emerges that the consent requested from the patients would not in any case comply with the requirements established by the regulations on the protection of personal data, as the interested party who intended to download the C-Healer App, in addition to entering some initial personal data (that is: name, surname, e-mail address and a personal password), he was forced, with a single acceptance key, also to read and tout court accept both the terms of use of the Application and the privacy information. The circumstance that a single disposition has been requested by the interested party determines the non-compliance with the requirement of the specific nature of the consent; this is even more so if we consider that the processing concerns health data, with respect to which, in addition to being specific, consent must also be explicit (Article 9, paragraph 2, letter a) of the Regulation). On this point, the aforementioned Guidelines 5/2020 on consent clarify two relevant aspects in relation to the case in question. On the one hand, that ""unequivocal positive action" means that the interested party must have taken a deliberate action to consent to the specific processing", on the other that "The data controller must (...) pay attention to the fact that consent cannot be obtained through the same action with which you accept a contract or the general conditions of service. The global acceptance of the general conditions of contract/service cannot be considered as an unequivocal positive action for the purposes of consent to the use of personal data" (see paragraphs 77 and 83). Given the above, the violation of the requirements of data protection legislation has been ascertained and in particular those relating to the need for consent to the processing of health data to be specific, informed and explicit (articles 5, paragraph 1 letter a), 6, 7 and 9 of the Regulation).

The evidence of the aforementioned violations also emerges with reference to the circumstance that the Association, during

the proceeding, has implemented a series of corrective measures precisely in order to make the treatments compliant with the regulatory framework on the protection of personal data. In particular, reference is made to the actions undertaken and described in the note of the XX. The Association, in fact, has foreseen punctual corrective interventions precisely in relation to the requirements relating to a specific, informed manifestation of consent and foreseeing that the system will generate two new requests for consent connected to the purposes referred to in the new text of the information. The first consent will concern the "Uploading of information on the state of health and the clinical picture of the user-patient on the C-Healer App, in pseudonymized mode, consequent to the request for assistance by the interested party and, more generally, facilitation of the dialogue between the same (requesting Patient User) and the Healthcare Professional User - Accepting Doctor, until the relative combination of these two subjects."; the second the "Communication of personal data of Patient Users, including those relating to health, to Healthcare Professional Users registered on the App, so that they can give their support and services, involving the connected archiving (these Professional Users, as mentioned above , from receipt onwards or in any case from the matching, will process the data as independent data controllers)".

The Association has also clarified that it has planned to be designated responsible for the treatment by health professionals pursuant to art. 28 of the Regulation with reference to the treatments carried out by them for the purpose of treatment and management of the relationship with the patient, by sending the model contract of appointment, in which the obligations and responsibilities of the parties are defined with respect to the roles assumed during the different phases of the treatment (see par. 5).

6.2 The principle of transparency and the information to be provided to data subjects (articles 5, paragraph 1, letter a), 12 and 13 of the Regulation)

Personal data must be processed in compliance with the principle of transparency (Article 5, paragraph 1 letter a) of the Regulations), providing the interested parties in advance - in the case of data collected directly from them - the information referred to in Article . 13 of the Regulation. This principle requires that information to data subjects relating to the processing of personal data be provided in a concise, transparent, intelligible and easily accessible form, with simple and clear language (cons. 39, 58 and art. 12 of the Regulation).

In this context, the obligation to provide data subjects with information in a "concise and transparent" form implies that the data controller presents the information in an effective and succinct manner, in order to avoid an information overload. They should

be "clearly differentiated from other information that does not concern private life, such as contractual clauses or general conditions of use" and should be "concrete and certain, should not be formulated in abstract or ambiguous terms nor leave room for multiple interpretations" (see points 8 and 12, of the Guidelines on transparency pursuant to regulation 2016/679, adopted by the Article 29 Working Party, on 29 November 2017, amended version adopted on 11 April 2018 and paragraph and paragraph 3.7).

In the context of applications that are capable of collecting large amounts of data from the device (for example data stored by the user and data from the mobile devices used to access the app), the end user has the right to know what type of personal data are being processed, for what purposes they are intended to be used and on the basis of which legal conditions. The availability of this information is in fact essential to request consent to the processing of the user's personal data, which can in fact be considered valid only if the interested party has been previously informed about the key elements of data processing and therefore made aware of the choices in the field of data processing that is being carried out through the manifestation of consent. Furthermore, the owner is required to communicate to the interested parties in simple and clear language whether the data can be reused by third parties and, if so, for what purposes. Generic indications present in the Association's documentation as "product innovation" are to be considered inadequate for informing users (see paragraph 3.7 of Opinion 02/2013, on applications for intelligent devices adopted on February 27, 2013).

In accordance with the principle of transparency, both the purposes and the corresponding legal bases of the processing must therefore be clear before the processing begins.

In this regard, it should be noted in particular that the information, in the version prior to the changes made by the Association, did not mention the different treatments and the different roles assumed by the Association and by health professionals in relation to the treatment of patients' personal data and did not indicate the legal basis on the basis of which the Association communicated patient data to the aforementioned health professionals.

With reference to the legal bases of the processing, the original information also contained a plurality of very heterogeneous indications and not specifically related to the purposes pursued. In fact, the following legal bases of the treatment were indicated "art. 6, par. 1, lit. a), b), c), d), and e) of the GDPR" without specifying for each of them which treatments they referred to.

In addition, despite the fact that the treatment, as declared by the Association itself, also concerns data relating to health (e.g.

blood pressure, blood sugar, allergies, intolerances, the presence of particular pathologies or the intake of certain drugs), the correct legal basis for the processing of such data and for their communication to the healthcare professionals who will take care of the patients, since the indication of the art. 9 of the Regulation concerning the conditions of lawfulness of the processing of particular categories of health data.

A contradiction was also found regarding the optional/mandatory nature of the provision of data on the health of the data subjects. While in the original information document and in the aforementioned acknowledgment note to the Authority's request for information, the Association declares that such information is provided spontaneously during registration, when creating an account or even subsequently, in the document in the document called "Terms of use and privacy policy", however, the provision of data is described as mandatory (see point 4).

Contradictory elements also emerge with reference to the exercise of the rights granted to data subjects by the Regulation, which in the health sector can be exercised with certain limitations which are not taken into account in the aforementioned information documents. In addition, the original disclosure also indicated the right to object "in any case when the processing takes place for direct marketing purposes, including profiling connected to such marketing", but there was no mention of such processing in the section relating to the purposes of the processing. On this point, it is also noted that, in the section relating to the "Methods of processing" of the original information, exactly the opposite was said, namely that "No automated decision-making processes, including profiling, are envisaged".

Further contradictions can be seen with reference to the circumstance that the original disclosure provided that the interested party could "revoke any consent given for specific purposes at any time, by forwarding a request to the Data Controller", although, as highlighted above, in the download process of the App, no consent was required with respect to the specific purposes of the processing pursued by the owner.

It should also be noted that with regard to data retention times and the transfer of data to a third country or to an international organization, what was indicated in the original disclosure was too vague. The scope of the data transfer and the retention period of the same must in fact be precisely identified with reference to the different types of data processed and the distinct processing activities indicated in the information.

Finally, the first version of the information examined did not indicate the contact details of the data protection officer as required by the Regulation.

Having said that, it has been ascertained that the disclosure model provided by the Association to interested patients who intend to use the services offered by the latter through the C-Healer App violates the principles of correctness and transparency pursuant to articles 5, par. 1, lit. a) 12 and 13 of the Regulation).

With reference to the violation profiles described above, during the proceeding the Association has put in place a series of corrective measures aimed at bringing the processing into line with the applicable regulatory provisions. In this regard, please refer to what is described in the previous paragraphs and in particular, to the actions described in the previous points 3.3. and 5.

6.3 Impact assessment (Article 35 of the Regulation)

On the basis of the non-shareable assumptions according to which the treatments in question did not involve the existence of high or high risks for the rights and freedoms of the users-interested parties and the requirement of the "large scale" could not even be considered configured, since the number of users-patients aborigine assigned to care for health professionals, did not appear to be more than 500 units, the Association did not carry out any impact assessment with respect to the treatments in question.

However, in light of the nature of the data processed and the potential number of interested parties, it is believed that the processing in question falls within the cases in which the data controller cannot disregard a prior impact assessment on data protection, pursuant to of the art. 35 of the Regulation and the criteria identified by the Group art. 29 in the Guidelines concerning "Guidelines on data protection impact assessment and determination of the possibility that the processing "may present a high risk" for the purposes of Regulation (EU) 2016/679, adopted on 4 April 2017 as amended and last adopted on 4 October 2017.

In particular, as already represented by the Authority in similar investigations, the case in question is one of those for which the controller is required to carry out, "before proceeding with the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data ” (art. 35 of the Regulation). This is because, for the treatment in question, there are certainly two of the criteria indicated by the European Data Protection Committee to identify the cases in which a treatment must be the subject of an impact assessment. In particular, reference is made to the following criteria: "data of a sensitive or highly personal nature", "data relating to vulnerable data subjects" including patients (see 4 Guidelines on impact assessment on the protection of data and determination of the possibility that the treatment "may present a high risk"

for the purposes of regulation (EU) 2016/679 adopted on April 4, 2017, as amended and most recently adopted on October 4, 2017 -WP 248 rev.01, III, letter B, points 4 and 7). With reference to the present case, the following criteria can also potentially be satisfied: "processing of data on a large scale", and "innovative use or application of new technological or organizational solutions" (see the aforementioned Guidelines, III, letter B, points 5 and 8) (see provisions of 12 March 2020, 21 April 2021 and 13 May 2021).

While acknowledging that the Association has represented that "the activities connected to the preparation of the aforementioned impact assessment are ending", the same, as owner of the data being processed, should have, before starting the processing operations, conduct the impact assessment pursuant to art. 35 of the Regulation.

6.4 The register of processing activities (Article 30 of the Regulation)

Although during the proceedings the Association demonstrated that the register of processing activities contained all the elements referred to in art. 30 of the Regulation, it is represented that the same, reporting the date of 17 January 2021 from the beginning, makes it clear that it was prepared by the Association only after the processing had begun, and therefore belatedly and therefore in violation of art. 30 of the Regulation. The keeping of the register is in fact an essential element for the governance of the treatments and for the effective identification of those at greater risk. The Association was required, also in homage to the principle of accountability, which permeates the renewed regulatory framework on the protection of personal data (Article 5, paragraph 2 of the Regulation) to adopt the aforementioned register at the same time as the start of operations treatment since the derogation from keeping the register envisaged by the Regulation does not operate in the presence of even only one of the elements indicated by art. 30, par. 5 (treatment that presents a risk to the rights and freedoms of the interested party, non-occasional treatment, treatment that includes particular categories of data pursuant to article 9 or data relating to criminal convictions and offences), which are, without doubt, present in the case in question (see provision of 17 December 2020, web doc. n. 9529527).

7. Conclusions

In the light of the assessments referred to above, taking into account the statements made by the owner during the investigation □ the truthfulness of which may be called upon to answer pursuant to art. 168 of the Code□ the elements provided by the data controller in the defense brief, although worthy of consideration, do not allow to overcome most of the findings notified by the Office with the deed of initiation of the procedure, since none of the cases envisaged apply by art. 11 of the

Regulation of the Guarantor n. 1/2019.

For these reasons, the illegality of the processing of personal data carried out by the Association in violation of articles 5, par. 1 lit. a), 6, 7, 9, 12, 13, 30 and 35 of the Regulation. The violation of the aforementioned provisions also renders the administrative sanction envisaged by art. 83, par. 4 and 5 of the Regulation, pursuant to articles 58, par. 2, lit. i), and 83, par. 3, of the same Regulation.

In this context, considering, in any case, that the conduct has exhausted its effects and that specific measures have been adopted to bring the treatment in question into compliance with the regulations in force regarding the protection of personal data, the conditions for the adoption of the corrective measures pursuant to art. 58, par. 2, of the Regulations.

8. 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; article 166, paragraph 7, of the Code).

The violation of the articles 5, par. 1 lit. a), 6, 7, 9, 12, 13, 30 and 35 of the Regulations, caused by the conduct put in place by the C-Healer Association is subject to the application of the administrative fine pursuant to art. 83, par. 4, lit. a) and 5, lett. a) and b) of the Regulation.

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 College [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).

The aforementioned pecuniary administrative sanction imposed, depending on the circumstances of each individual case, must be determined in the amount taking into account the principles of effectiveness, proportionality and dissuasiveness, indicated in art. 83, par. 1, of the Regulation, in the light of the elements provided for in art. 83, par. 2 and, of the Regulation in relation to which it is observed that:

1. the processing carried out concerned information suitable for detecting the state of health of around 550 data subjects (Article 4, paragraph 1, no. 15 of the Regulation and Article 83, paragraph 2, letters a) and g) of the regulation);

2. the data controller is a non-profit voluntary association with no commercial, industrial or political purpose, as can be clearly

found in its Articles of Association and Articles of Association, whose management report, relating to the year 2021, is substantially balanced and carried out the treatment in question at a particularly critical moment in order to provide advice and/or health care to patients suffering from Covid-19 on the basis of their consent (Article 83, paragraph 2, letter k) of the Regulation) ;

3. following the start of the investigation by the Office, the Association ordered the immediate interruption of the operation of the App, still suspended, which therefore remained active only for a little over a month (from 24 December 2021 to 5 February 2022), this in order to mitigate the potential negative consequences for the data subjects (Article 83, paragraph 2, letter c) of the Regulation);

4. the Association has put in place multiple measures aimed at bringing the processing of personal data into line with the current regulatory framework on the protection of personal data (Article 83, paragraph 2, letter c) of the Regulation);

5. there are no previous relevant violations committed by the data controller, nor have measures pursuant to art. 58 of the Regulation (art. 83, paragraph 2, letter e) of the Regulation);

6. the Association has fully collaborated with the Authority during the investigation and in the present proceeding (Article 83, paragraph 2, letter f) of the Regulation);

7. no complaints have been received pursuant to art. 77 of the Regulation, to the Guarantor on the incident.

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction provided for by art. 83, par. 5, letter. a) of the Regulations, in the amount of € 5.00,00 (five hundred) for the violation of the articles 5, par. 1 lit. a), b) and f), 6, 7, 9, 12, 13 and 27 of the Regulation, as a pecuniary administrative sanction withheld, pursuant to art. 83, par. 1 and 3, of the Regulation, effective, proportionate and dissuasive.

It is also believed that the ancillary 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, also in consideration of the type of personal data subject to unlawful processing.

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.

ALL THIS CONSIDERING THE GUARANTOR

declares the unlawfulness of the processing of personal data carried out by the Covid-Healer ODV Association, based in

Bolzano, Viale Stazione n. 7 (C.F. and P. IVA 03130830213), the violation of the articles 5, par. 1 lit. a), 6, 7, 9, 12, 13, 30 and 35 of the Regulation in the terms indicated in the justification.

ORDER

pursuant to articles 58, par. 2, lit. i) and 83 of the Regulation, as well as art. 166 of the Code, the Covid-Healer Association to pay the sum of 5.00.00 (five hundred) euros as an administrative fine for the violations indicated in this provision. 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

To the Covid-Healer Association to pay the sum of €5.00.00 (five hundred) 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 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 n. 689/1981.

HAS

pursuant to art. 166, paragraph 7, of the Code, the entire publication of this provision on the website of the Guarantor and believes that the conditions set forth in 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.

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, 20 October 2022

PRESIDENT

Station

THE SPEAKER

Zest

THE DEPUTY SECRETARY GENERAL

Philippi