

[doc. web no. 9832838]

Injunction against Sportitalia, a limited liability amateur sports club - 10 November 2022

Register of measures

no. 369 of 10 November 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter, the "Regulation");

HAVING REGARD TO the Code regarding the protection of personal data, containing provisions for the adaptation of the national legal system to Regulation (EU) 2016/679 (legislative decree 30 June 2003, n. 196, as amended by legislative decree 10 August 2018, n. 101, hereinafter "Code");

HAVING REGARD to the report presented on 15 May 2019 by SLC CGIL against Sportitalia, an amateur sports club with limited liability;

HAVING EXAMINED the documentation in the deeds;

HAVING REGARD TO the observations made by the general secretary pursuant to art. 15 of the Guarantor's regulation n. 1/2000;

SPEAKER Prof. Geneva Cerrina Feroni;

WHEREAS

1. The report to the Company and the outcome of the inspections.

With a report dated May 15, 2019, the SLC CGIL complained that, starting from October 2018, at the Get Fit Clubs in Milan managed by Società Sportitalia, a limited liability amateur sports club (hereinafter, the Company), "it is a clocking system was introduced for attendance, with a biometric terminal (fingerprint detection) for all employees and collaborators in order to register access and attendance at the Clubs".

The introduction of the biometric system, arranged despite the request made to the Company by the reporting organization, to

adopt "less invasive means - choosing non-biometric procedures", would have occurred in violation of the principles of lawfulness, necessity and proportionality.

On 5 September 2019, the Authority sent the Company an invitation to provide feedback on the facts being reported and, on 10 January 2020, as no response was received, a request for information pursuant to art. 157 of the Code.

Since the Company did not send any response in this case either, the Authority delegated the special privacy and technological fraud unit of the Guardia di Finanza to notify the act of initiation of the sanctioning procedure, pursuant to art. 166, paragraph 5, of the Code, in relation to the alleged violation of the same art. 166, paragraph 2 (where it establishes that the violation of article 157 of the Code is subject to the application of the administrative sanction pursuant to article 83, paragraph 5, of the Regulation). The Unit was also delegated to acquire the information already requested from the Company in relation to the facts being reported.

On 28, 29 and 30 September 2021, inspections were carried out at the company's registered office, during which, in addition to the notification of the initiation of the sanctioning procedure for the violation of art. 166, paragraph 2 of the Code, the following statements were recorded in the minutes:

to. at the company's registered office and at the 7 local units ("club with GET-FIT brand sign") "at present [...] a biometric detection system for employee attendance has been installed and is active [...]" (see report 28/9/2021, p. 3);

b. as regards the initiation of the sanctioning procedure subject to notification, the acknowledgment note to the Guarantor's request for information had also been prepared with the help of the Data Protection Officer on 16 October 2019 and entrusted for shipment via Pec to a employee of the company "who terminated the employment relationship in March 2021"; only following the notification of the act of initiation of the sanctioning procedure did the Company learn "that this communication was never sent [...]. The further communication from the Guarantor, sent by certified email on 10 January 2020, although it was delivered and received by the employee in charge of corporate correspondence, appears not to have been sent to the employee [...] in charge of this task (who should then have forward it to the DPO for the necessary comparison), for a sending error that was not detected or highlighted" (see report 29/9/2021, p. 5);

c. the dates of the installation of the biometric detectors at the registered office and at the offices of the 7 GET-FIT clubs in Milan were provided (between 2-3 October 2018 and, in one case, 4 September 2020); in this regard, the Company specified that "after the initial phase of preliminary operating tests, which took place at the Head Office starting from 1 October 2018, the

actual start of the treatment took place for all clubs from 8 October 2018 with the first surveys, while for that of via Pinerolo from 8 September 2020" (see report cited, p. 6);

d. the requirement of lawfulness of the treatments carried out "is based on the specific and free consent expressed by each individual employee" (see report cited, p. 6);

And. in this regard, the Company has delivered some documents bearing a "Privacy information for employees", which also bears at the bottom a signature for acknowledgment and consent to the processing of biometric data by the employee, dated 8 September 2021 and 16 October 2018, relating to three employees (see Annex 9, report cited, p. 6);

f. "to date, the company makes use of the collaboration of 132 employees, all affected by the processing in question"; furthermore "the system has been set up, in terms of hardware and software, to operate with the alternative badge method without the use of the biometric data", although no employee has requested to be able to use the alternative system (see aforementioned report, p. 7);

g. the data contained in the biometric reader can be accessed, by entering a password, by employees with the role of "Club Manager" and, at the administrative office, by the IT systems officer (see report of 30 September 2021, p. 9);

h. the biometric system produced by Kronotech s.r.l. and provided by Cronos s.r.l., treats "only the biometric model (template) which is created following processing upon registration of the biometric identification account of each user" (see aforementioned report, p. 9);

the. "the newly hired employee is entered in the KEROS registry, by the administration office, to which personal access credentials are issued [...] useful for managing one's work account (attendance, absence, receipts, hours worked , requests for permits, etc.)" (see report cited, p. 9);

j. subsequently "the biometric identity is created (enrollment), with the association of the aforementioned numerical code to the biometric model (template) which is generated following registration via fingerprint, of which the relative template remains only memorized in the physical device [...] present in the assigned club"; moreover "all 9 devices [...] are connected, by the various clubs, to a network via company VPN with ethernet cable, as the server in the central office [...] queries said biometric terminals in the remote offices on a daily basis to centralize the data relating to attendance and then send them, via FTP protocol [...] to a CRONOS srl server with the aim of combining these data with the personal data of the employees" (see report cited, p. 10);

k. the method of comparison at the time of authentication by the employee is of the "one to many" type (see report cited, p. 10);

L. "there is no logging of raw biometric data"; moreover, in relation to storage times, "when an employee terminates the employment relationship with the company [one] proceeds to request the termination, via e-mail, of the relative personal registry user to Cronos support, for the subsequent task" (see report cit., p. 10).

On 14 October 2021, the Company sent further documentation to resolve the reserves presented at the end of the inspection activities, in particular a copy of the register of processing activities carried out by the Company, without date and in any case, as indicated, "updated to 31.07 .21". The Company also represented that "for the detection of personnel attendance and access, in addition to [the] biometric system, a detection system is also active through the use of a badge".

2. The initiation of the proceeding and the deductions of the Company.

Given that, as already reported in the previous paragraph, during the inspections, the Special Privacy and Technological Fraud Unit of the Guardia di Finanza notified the deed of initiation of the sanctioning procedure in relation to the alleged violation of the same art. 166, paragraph 2 (with regard to art. 157 of the Code), on 3 March 2022 the Office carried out, pursuant to art. 166, paragraph 5, of the Code, a new notification to the Company of the alleged violations of the Regulation found, with reference to articles 5, par. 1, lit. a), 9, 13, 30, para. 1, lit. c) of the Regulation.

With defense briefs dated April 2, 2022, the Company stated that:

to. "the system for detecting biometric data of employees, [...] has the sole purpose of detecting the presence of employees in order to facilitate the registration of entry and exit times";

b. since "very often in the past [...] employees forgot to register, through the use of the badge, their arrival or their exit from the workplace, a circumstance that forced the employer to take disciplinary measures [...] it was decided to adopt this system, which is much leaner and faster";

c. in relation to the biometric detection system "all employees [...] have given their free, specific and written consent";

d. "employees are in any case informed of the possibility of not giving their consent to the processing of biometric personal data or of being able to revoke it at any time";

And. the Company has therefore acted "in total good faith and transparency [and] if there has been a violation, it can only be considered to be culpable";

f. in any case "with a view to total collaboration with the Privacy Guarantor, it is confirmed [...] that with effect from next May 2, 2022, the use of the biometric data collection system will be discontinued for employee access with contextual cancellation of any data possibly acquired and only the traditional registration system will be used [...] through the use of the "badge".

Finally, during the hearing held on 6 June 2022, the Company declared that:

to. "as soon as it received notification of the violations from the Authority [the company] decided to stop using the system. In particular, it is confirmed that the fingerprint detection system has been deactivated since May 2";

b. "Cronos s.r.l., the company that [...] supplied the system, has not [...] communicated any problematic aspect relating to the applicability of this system [...]. The total good faith of the company is therefore underlined";

c. "at the same time as the abandonment of the biometric system, the company asked Cronos s.r.l. to delete the collected data given that the extracted templates were stored only in the database of the company providing the service, while only the entry and exit data from the workplace were visible to the personnel office";

d. "when the contract with Cronos s.r.l. the company had not yet appointed the DPO. When the first request for information from the Guarantor arrived, in 2019, a response was prepared by the company which was also sent for viewing to the DPO who, on the occasion, raised some objections to the system (in this regard, please refer to the exchange of e- e-mail referred to in attachment 3 of the inspection report). However, this response was never sent to the Guarantor due to the failure to send it by an employee responsible for this, who then resigned. As regards the second request for information sent by the Guarantor, the failure to respond is attributable to a mere oversight";

And. "the biometric data have not been processed continuously since the introduction of the aforementioned detection system (about four years) considering that the gyms have been closed for almost a year due to the pandemic and that even after the reopening some employees remained on layoffs , while others resigned. Therefore the number of employees was lower than those in force at the time of activation of the system";

f. "We are coming out of a disastrous period especially for gyms and the Guarantor is asked to take this into account when making its assessments given that the financial situation of the sector in general and of society in particular is still particularly difficult".

3. The outcome of the investigation.

3.1. The processing of biometric data carried out by the company.

As a result of the examination of the declarations made to the Authority during the proceeding as well as of the documentation acquired, it appears that the Company, as owner, has carried out some processing operations, referring to its employees, which are not compliant with the regulations in matter of personal data protection.

In this regard, it should be noted that, unless the fact constitutes a more serious offence, anyone who, in a proceeding before the Guarantor, falsely declares or attests news or circumstances or produces false deeds or documents, is liable pursuant to art. 168 of the Code "False statements to the Guarantor and interruption of the performance of the duties or exercise of the powers of the Guarantor".

On the merits, it emerged that the Company has carried out, starting from the month of October 2018, processing of personal data of its employees through the activation of a biometric system, aimed at verifying the presence in service, based on the detection of the fingerprint and the association of the fingerprint to a code assigned to the employee, in order to "help employees register their entry and exit times" and adopt a "leaner and faster" system than the one previously in use based on badges.

The treatment concerned a significant number of data subjects, equal to 132 employees, although in some periods of health emergency the number of workers involved in the biometric treatment was significantly lower.

The only information provided to employees regarding the processing of biometric data is contained in a short paragraph present within the information relating to the general nature of the processing carried out in the context of the employment relationship; moreover, the register of processing activities dated 31 July 2021 does not include biometric data among the types of data processed by the controller.

It is acknowledged that, according to what was declared by the Company, on 2 May 2022 the biometric system was replaced by a non-biometric attendance recording system.

Finally, it emerged that the Company did not respond to the request for information formulated by the Authority pursuant to art. 157 of the Code.

The processing of personal data carried out by the Company, subject to verification, concerned the biometric data of the employees, given that, as clarified by the Authority, this type of data is processed both in the registration phase (so-called enrollment, consisting in the acquisition of the biometric characteristics - in this case fingerprints - of the interested party (see points 6.1 and 6.2 of attachment A to the provision of the Guarantor of 12 November 2014, n. 513, in www.garanteprivacy.it,

web doc. n. 3556992) , both in the biometric recognition phase, when detecting attendance (see also point 6.3 of attachment A to the aforementioned provision).

This also in the light of the definition of biometric data provided by the Regulation ("personal data obtained from a specific technical treatment relating to the physical, physiological or behavioral characteristics of a natural person which allow or confirm its unique identification, such as the facial image or dactyloscopic data", art. 4, n. 14, of the Regulation) which has also included this type of data among the "particular data" (art. 9, paragraph 1 of the Regulation).

3.2. Violation of articles 5, par. 1, lit. a) and 9 of the Regulation.

The Company has delivered copies of some documents, containing a "Privacy Policy for employees", referring to the generality of the treatments carried out in the context of the employment relationship with the Company, which finally, at the bottom of the section "Having read the employee - Consent to processing", where the following sentence also appears: "As regards the processing of my biometric data (fingerprint) for the monitoring and recording of accesses/exits, which the Data Controller will treat with the utmost attention and with the use of suitable computer systems, with this signature I give my express consent to the aforementioned processing for the purposes indicated", bears the date and signature of the employee (the copies provided refer to three employees; see Annex 9, report of operations performed).

In this regard, it should be noted that, based on the regulations governing the protection of personal data, the processing of biometric data (as a rule prohibited pursuant to the aforementioned article 9, paragraph 1 of the Regulation) is permitted only if one of the conditions indicated by the art. 9, par. 2 of the Regulation and, with regard to treatments carried out in the workplace, only when the treatment is "necessary to fulfill the obligations and exercise the specific rights of the data controller or of the interested party in the field of labor law and social security and protection social security, to the extent that it is authorized by Union or Member State law or by a collective agreement under the law of the Member States, in the presence of appropriate guarantees for the fundamental rights and interests of the data subject" (Article 9 , paragraph 2, letter b), of the Regulation; v. as well, art. 88, par. 1 and cons. 51-53 of the Regulation).

Therefore, although in the working context the purposes of detecting employee attendance and verifying compliance with working hours may fall within the scope of application of art. 9, par. 2, lit. b) of the Regulation as they imply a treatment "necessary to fulfill the obligations and exercise the specific rights of the data controller or of the interested party in the field of labor law [and social security and social protection]" (see also art. 88, paragraph 1, Regulation), however the processing of

biometric data will be permitted only "to the extent authorized by the law of the Union or of the Member States [...] in the presence of appropriate guarantees for the fundamental rights and interests of the 'interested party' (Article 9, paragraph 2, letter b), and cons. nos. 51-53 of the Regulation).

In this framework, in order for a specific treatment involving biometric data to be lawfully initiated, it is therefore necessary that the same find its basis in a regulatory provision that has the characteristics required by the data protection regulations, also in terms of proportionality of the regulatory intervention with respect to the aims to be pursued.

The current regulatory framework also provides that the processing of biometric data, in order to be lawfully implemented, takes place in compliance with "further conditions, including limitations" (see Article 9, paragraph 4, of the Regulation).

This provision has been implemented, in the national legal system, with the art. 2-septies (Guarantee measures for the processing of genetic, biometric and health-related data) of the Code.

The rule provides that the processing of these categories of data is lawful when one of the conditions referred to in art. 9, par. 2, of the Regulation "and in compliance with the guarantee measures established by the Guarantor", in relation to each category of data.

The employer, data controller, is, in any case, required to respect the principles of "lawfulness, correctness and transparency", "purpose limitation", "minimization" as well as "integrity and confidentiality" of data and "accountability" (Article 5 of the Regulation). The data must also be "processed in such a way as to guarantee adequate security" of the same, "including protection, through appropriate technical and organizational measures, against unauthorized or unlawful processing and against accidental loss, destruction or damage" (art. 5, paragraph 1, letter f), and art. 32 of the Regulation).

In this latter regard, it is also noted that the use of biometric data in the context of the ordinary management of the employment relationship (such as the activity of detecting attendance), for the declared purpose of guaranteeing greater speed and streamlining of the relative operations against of repeated forgetting in stamping with a badge, does not appear to comply with the principles of minimization and proportionality of the treatment (Article 5 of the Regulation).

In the light of the aforementioned regulatory framework, the processing of biometric data carried out by the Company appears to have been carried out in the absence of an appropriate legal basis given that the collection of consent from the interested parties, in the context of the employment relationship, does not correspond to what is established by the aforementioned art. 9, par. 2, lit. b) of the Regulations in the terms set out above.

Furthermore, it should be noted that the Authority with its own provisions considered that, in general terms, the consent of the worker does not normally constitute a valid prerequisite for lawfulness for the processing of personal data in the workplace, regardless of the public nature or of the employer, this in the light of the asymmetry between the respective parts of the employment relationship and the consequent, possible, need to ascertain from time to time and concretely the effective freedom of the expression of will of the employee (see, among the others, provision n. 16 of 14 January 2021, web doc. n. 9542071; n. 35 of 13 February 2020, web doc. n. 9285411; n. 500 of 13 December 2018, web doc. n. 9068983 ; see also articles 6-7 and recitals 42-43, Regulation (EU) 2016/679; see also, in a compliant sense, Article 29 Group, Guidelines on consent pursuant to EU Regulation 2016/679 - WP 259 - of 4 May 2020, spec. paragraph 3.1.1.; Opinion 2/2017 on the processing of data in the workplace, WP 249, spec. par. 3.1.1 and 6.2).

However, it is noted that the Company has interrupted the processing of biometric data starting from 2 May 2022, declaring under its own responsibility that it has also ordered the cancellation of the data collected.

The Company, for the above reasons, has therefore violated the articles 5, par. 1, lit. a) and 9, par. 2, lit. b) of the Regulation, from the date of installation and commissioning of the devices, as shown in the documents, to the date of 2 May 2022.

3.3. Violation of articles 5, par. 1, lit. a) and 13 of the Regulation.

The data controller must process the data "lawfully, correctly and transparently" (Article 5, paragraph 1, letter a) of the Regulation), adopting "appropriate measures to provide the interested party with all the information referred to in the articles 13 and 14 [...]" (art. 12 of the Regulation).

As a result of the preliminary investigation, it emerged that the only information elements provided by the Company in relation to the processing of biometric data of employees are those contained in the aforementioned "Information on privacy for employees" (specifically the following: "the Data Controller will deal with utmost care and with the use of suitable IT systems [i] biometric data (fingerprint) for monitoring and recording accesses/exits").

These elements are completely unsuitable to represent the characteristics of the treatment that is intended to be carried out through the specific biometric devices, as prescribed by art. 13 of the Regulation (in particular, with regard to the specific case: data controller and processor, legal basis, retention times, rights of the interested party, right to lodge a complaint with a supervisory authority).

Moreover, with specific regard to the legal basis of the processing, in the document prepared by the Company there is no

reference to the possibility of using, as an alternative to the biometric system, the traditional system based on the badge or to be able to revoke the consent given, as declared by the Company itself during the investigation process.

In the context of the employment relationship, the obligation to inform the employee is also an expression of the duty of correctness pursuant to art. 5, par. 1, lit. a) of the Regulation.

The Company, for the above reasons, has therefore violated the articles 5, par. 1, lit. a) and 13 of the Regulation, from the date of installation and commissioning of the devices, as shown in the documents, to 2 May 2022.

3.4. Violation of the art. 30, par. 1, lit. c) of the Regulation.

The outcome of the verification activity also revealed that the register of processing operations prepared by the Company, dated 31 July 2021, does not indicate biometric data among the types of data processed by the controller (see documentation sent on 14/10/ 2021).

Considering that the register is a tool that allows the owner, in the context of the c.d. responsibility ("accountability": art. 5, paragraph 2, of the Regulation), to have an updated picture of the treatments carried out also in view of the risk analysis as well as to be able to respond to requests for exhibition by the supervisory authority , the contents reported therein must correspond to the treatments actually in place.

For this reason, the Authority considered that the register must be compiled in such a way as to indicate the verifiable date of its first establishment and that of the last update (see FAQ on the register of processing activities, n. 5). This taking into account the fact that keeping the register does not constitute a formal fulfillment but an integral part of a system of correct management of the processing of personal data carried out.

Therefore, the failure to take into consideration, within the register, the processing of biometric data of employees results in violation of the provisions of art. 30 par. 1, lit. c), of the Regulation, according to which the description of the categories of personal data being processed must also be present in the register of processing activities carried out by the owner under his own responsibility.

3.5. Violation of the art. 157 in relation to the provisions of art. 166, paragraph 2, of the Code.

Finally, it has been ascertained that the Company has failed to respond to the requests for information addressed by the Authority, in particular to the invitation of 5 September 2019 and to the request made pursuant to art. 157 of the Code, sent on 10 January 2020 (containing the express notice that "in case of non-compliance with this request, the pecuniary administrative

sanction provided for by art. 166, paragraph 2 of the Code must be applied"), despite the communications of the offices of the Guarantor had been duly notified.

On the basis of the aforementioned article 157 of the Code "Within the scope of the powers referred to in article 58 of the Regulation, and for the performance of its duties, the Guarantor may request the holder [...] to provide information and produce documents". The art. 166, paragraph 2, of the Code establishes that the violation of art. 157 of the Code is subject to the administrative sanction pursuant to art.83, par. 5, of the Regulation. The failure of the Company to respond to the Guarantor's request for information therefore occurred in violation of art. 157 of the Code in relation to the provisions of art. 166, paragraph 2, of the Code, with consequent application of the administrative sanction pursuant to art.83, par. 5, of the Regulation.

4. Conclusions: declaration of illegality of the treatment. Corrective measures pursuant to art. 58, par. 2, Regulation.

For the aforementioned reasons, the Authority believes that the declarations, documentation and reconstructions provided by the data controller during the investigation do not allow the findings notified by the Office to be overcome with the act of initiating the procedure and are therefore unsuitable for allow the filing of this proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

The processing of personal data carried out by the Company and in particular the processing of biometric data of employees and the failure to respond to the Guarantor's request for information is in fact illegal, in the terms set out above, in relation to articles 5, par. 1, lit. a), 9, 13, 30, para. 1, lit. c) of the Regulation and 157 of the Code.

The violation ascertained in the terms set out in the reasoning cannot be considered "minor", taking into account the nature, gravity and duration of the violation itself, the degree of responsibility and the manner in which the supervisory authority became aware of the violation (cons. 148 of the Regulation).

Therefore, given the corrective powers attributed by art. 58, par. 2 of the Regulation, the application of a pecuniary administrative sanction pursuant to art. 83 of the Regulation, commensurate with the circumstances of the specific case (Article 58, paragraph 2, letter i) of the Regulation).

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

At the end of the proceeding it appears that Sportitalia, an amateur sports club with limited liability has violated the articles 5, par. 1, lit. a), 9, 13, 30, para. 1, lit. c) of the Regulation and 157 of the Code. For the violation of the aforementioned provisions,

the application of the pecuniary administrative sanction envisaged by art. 83, par. 4, lit. a) and par. 5, letter. a) and b) of the Regulation, through the adoption of an injunction order (art. 18, law 11.24.1981, n. 689).

Considering it necessary to apply paragraph 3 of the art. 83 of the Regulation where it provides that "If, in relation to the same treatment or related treatments, a data controller [...] violates, with willful misconduct or negligence, various provisions of this regulation, the total amount of the pecuniary administrative sanction does not exceed amount specified for the most serious violation", the total amount of the fine is calculated so as not to exceed the maximum prescribed by the same art. 83, par. 5. With reference to the elements listed by art. 83, par. 2 of the Regulation for the purposes of applying the pecuniary administrative sanction and the relative quantification, taking into account that the sanction must "in any case [be] effective, proportionate and dissuasive" (Article 83, paragraph 1 of the Regulation), it is represented that In the present case, the following circumstances were considered:

a) in relation to the nature, gravity and duration of the violation (which lasted for just under four years, from the date of activation of the devices, which occurred for all clubs on 10/08/2018 and, in one case, the 8/9/2020, until 2/5/2022) the nature of the violation which concerned the general principles of treatment was considered relevant;

b) with reference to the intentional or negligent nature of the violation and the degree of responsibility of the owner, the conduct of the Company and the degree of responsibility of the same was taken into consideration which did not comply with the regulations on data protection, in relation to a plurality of provisions also concerning the general principles of processing (lawfulness and correctness);

c) in favor of the Company, the cooperation with the Supervisory Authority and the absence of previous relevant violations were taken into account.

It is also believed that they assume relevance in the present case, taking into account the aforementioned principles of effectiveness, proportionality and dissuasiveness with which the Authority must comply in determining the amount of the fine (Article 83, paragraph 1, of the Regulation), in firstly the economic conditions of the offender, determined on the basis of the revenues achieved by the company with reference to the condensed financial statements for the year 2021, as well as the particular economic context linked to the health emergency. Lastly, the extent of the sanctions imposed in similar cases is taken into account.

In the light of the elements indicated above and the assessments made, it is believed, in the present case, that the

administrative sanction of payment of a sum equal to 20,000 (twenty thousand) euros should be applied against Sportitalia, an amateur sports club with limited liability.

In this context, it is also considered, in consideration of the type of violations ascertained that concerned the general principles of treatment, that pursuant to art. 166, paragraph 7, of the Code and of the art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019, this provision must be published on the Guarantor's website.

It is also believed that the conditions pursuant to art. 17 of Regulation no. 1/2019.

ALL THAT BEING CONSIDERED, THE GUARANTOR

notes the illegality of the processing carried out by Sportitalia, an amateur sports club with limited liability, in the person of its legal representative, with registered office in Via Giuseppe Meda, 52, Milan (MI), Tax Code 09600560966, pursuant to art. 143 of the Code, for the violation of the articles articles 5, par. 1, lit. a), 9, 13, 30, para. 1, lit. c) of the Regulation and 157 of the Code;

ORDER

pursuant to art. 58, par. 2, lit. i) of the Regulations to Sportitalia, an amateur sports club with limited liability, to pay the sum of 20,000 (twenty thousand) euros as an administrative fine for the violations indicated in this provision;

ENJOYS

then to the same Company to pay the aforementioned sum of 20,000 (twenty thousand) euros, according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of adopting the consequent executive deeds pursuant to art. 27 of the law n. 689/1981. It should be remembered that the offender retains the right to settle the dispute by paying - always according to the methods indicated in the attachment - an amount equal to half of the fine imposed, within the term set out in art. 10, paragraph 3, of Legislative Decree lgs. no. 150 of 1.9.2011 envisaged for the lodging of the appeal as indicated below (art. 166, paragraph 8, of the Code);

HAS

the publication of this provision on the Guarantor's website pursuant to art. 166, paragraph 7, of the Code and of the art. 16, paragraph 1, of the Guarantor Regulation n. 1/20129, and believes that the conditions pursuant to art. 17 of Regulation no. 1/2019.

Pursuant to art. 78 of the Regulation, as well as articles 152 of the Code and 10 of Legislative Decree no. 150/2011, opposition

to the ordinary judicial authority may be lodged against this provision, with an appeal lodged with the ordinary court of the place identified in the same art. 10, within the term of thirty days from the date of communication of the measure itself, or sixty days if the appellant resides abroad.

Rome, 10 November 2022

PRESIDENT

station

THE SPEAKER

Cerrina Feroni

THE SECRETARY GENERAL

Matthew