SEE ALSO NEWSLETTER OF FEBRUARY 19, 2021

[doc. web no. 9542071]

Injunction order against the Provincial Health Authority of Enna - 14 January 2021

Register of measures

no. 16 of 14 January 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

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

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national legal system to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons with regard to the processing of personal data, as well as to the free movement of such data and which repeals Directive 95/46/EC (hereinafter the "Code");

CONSIDERING the Regulation n. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved with resolution no. 98 of 4/4/2019, published in the Official Gazette no. 106 of 8/5/2019 and in www.gpdp.it, doc. web no. 9107633 (hereinafter "Regulation of the Guarantor n. 1/2019");

Given the documentation in the deeds;

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

Speaker the lawyer Guido Scorza;

WHEREAS

1. Premise.

With reference to press articles published in November 2019 which reported the news that the Provincial Health Authority of

Enna (hereinafter "the Company") had adopted, in its offices, a system that allows the processing of employee biometric data for attendance tracking, in order to ensure "greater technical reliability in verifying the identity of each employee" and "discourage [re] absenteeism [...]", the Office has launched an investigation against the Company .

2. The preliminary investigation.

In response to the specific requests of the Office (see note of the XX, prot. n. XX in the documents), the Company, with a note of the XX, specified that:

- the same "provides its services in 21 Municipalities belonging to the province of Enna and […] of Messina. The company's employees [...] are over 2000 and work in 4 hospitals [...] as well as in the outpatient clinics and territorial offices located in 22 Municipalities";

- the administration has introduced "the biometric identity verification system" as "the existence of decentralized controls [...] and the type of activity performed (several operators perform their activities over two and/or three shifts in the 24 hours, sometimes even in hospitals and territorial facilities) involves considerable complexity in the management of employee personnel" and therefore the system was activated "in the light of the provisions of law no. 56/2019";

- the system uses "software capable of acquiring the employee's data and storing them in encrypted form on a secure device (badge) given exclusively to the interested party";

- "the software provides, immediately after the phase of registration in encrypted form of the data, to their cancellation";

- "all employees have been provided with information pursuant to art. 13 of the Regulation";

- the data registration procedure involves the "detection of the biometric fingerprint which is transformed into an encrypted string, which is in turn memorized in the badge"

- the reading of the data, upon detecting the presence, takes place through the simultaneous use of the badge (which must be brought close to the presence detector) and by placing the finger on the device: "the system compares locally and only for the time necessary to verification, string stored in the badge with the one temporarily calculated by the presence detector" and, if the comparison coincides, "the temporarily calculated string is automatically deleted [...] no biometric data is stored", but "only the employee's matriculation number , the time and date of attendance";

- "no video surveillance system has been installed in the various company entrances"; and for all these reasons, the Company maintains that "there are no critical issues or violations of the rules". These considerations are also contained in a document

called "impact assessment".

With a note of the XX (prot. n. XX), the Office, on the basis of the elements acquired, notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation, inviting the aforesaid owner to produce defense writings or documents to the Guarantor or to ask to be heard by the Authority (art. 166, paragraphs 6 and 7, of the Code; as well as art. 18, paragraph 1, of law no. 689 of 11/24/1981).

With the note mentioned above, the Office found that the Company processes, in the manner described above, biometric data of employees for the purpose of detecting attendance in violation of the principle of "lawfulness, correctness and transparency", art. 5, par. 1, lit. a), of the Regulation and in the absence of a suitable prerequisite of lawfulness, in violation of articles 6, par. 1, lit. c) and 9 par. 2, lit. b), and par. 4, of the Regulation.

With note dated XX, the Company sent its defense briefs, stating, among other things, that:

- there would be no processing of personal data by the administration as "the processing of the data subject's personal data [would] be carried out by the latter" and "must be considered per se lawful and legitimate pursuant to national and the Community one, without the conditions and any limitations sanctioned by articles 5, 6 and 9 of the Regulation having to (or being able) to be applied to it", similarly to what happens for "the processing of one's own fingerprint stored on a specific device , as a tool for accessing the same (whether it is the subject's own computer or smartphone) [which] is beyond any application of national and Community legislation" (see pp. 4 and 5);
- "in the present case, all the conditions certainly exist for concluding that, when the employee's identity is verified at the access points, there is actually a processing of biometric personal data [but that the same is not] subject to the provisions of the Regulations and of the Code" and "consequently outside the competence of the Guarantor Authority;
- this because "the processing is carried out directly and personally by the interested party [...] the entire mechanism is specifically set up so as to prevent a person other than the interested party from processing the biometric data of the interested party [...] the processing of the biometric data begins (in an automated way) if and when (and only when) the employee starts the process by performing two material operations that are under his personal and exclusive control: a. Placing the badge on the reader and b. The rest of the fingertip on the scanner. Once these operations have been completed, the process of surveying and comparing the data begins" (pp. 7 ss.)
- "these simple gestures have a unique meaning expressive of a precise will of the employee to initiate and therefore, in a

certain sense, to consent to the processing of data";

- "during the comparison between the stored biometric data and that detected by the scanner, the reader does not communicate with other systems or machines and there is therefore no possibility that the biometric data which at that moment are found (albeit for very few instants) inside of the machine are acquired, memorized, altered, or treated in any way by third parties. To do this, in fact, it would be necessary to physically access the machine in the same short period of time in which the comparison of the data takes place - a period of time in which, however, the data subject is in direct physical contact with the machine itself which is , therefore, under its direct control";

- "the entire biometric data processing process never takes place and can never take place under the direct or indirect control of the administration because it takes place under the direct and exclusive control of the employee and is, indeed, expressly aimed at preventing others from subjects who are not the interested party can have any access to the personal and biometric data of the same" (p. 9);

- in any case - if it is believed that the processing falls within the scope of application of the Regulation - "the purpose pursued by the adoption of biometric systems for detecting attendance responds to an extremely topical need aimed at preventing crimes against the public administration and, in general, incorrect behavior on the part of employees, in itself capable of considerably reducing the efficiency of the Public Administration. Where, as in the present case, the public administration concerned operates in the field of health care, two distinct pivotal interests of both national (art. 32 and art. 97 Constitution of the Republic) and community (art. 35 and article 41 of the Charter of Fundamental Rights of the European Union): the right to health and the principle of good administration" (p.11);

- "in recent years, various public administrations have made the same choice of adopting a biometric verification system of attendance without encountering, as far as the inferring Company is aware, any objection by the aforementioned Authority [...] from induce in the general conviction of the lawfulness of the behavior [...] "the Privacy Guarantor, with provision of 15 September 2016 n. 357, expressed a positive opinion with reference to the preliminary request [from a hospital ...] for the installation of the biometric data reading system (fingerprints) for detecting the presence of employees on duty [...with] operating modes [similar to those in use] at the ASP of Enna" (p. 16);

- "the existence of a legal obligation dating back to l. 56/2019 [...although subject] to numerous critical remarks regarding the compatibility of this national rule with the Community regulatory context [...] leads to the exclusion that in the present case the

ASP of Enna can be accused of a violation of art. 6";

- "the administration concerned, therefore, can only adapt to what (the Guarantor Authority itself) deems to be an obligation legally imposed in the face of the existence of mere doubts on the compatibility of said obligation with some of the criteria dictated by the Regulation (doubts that moreover, the Administration does not believe it can agree except to the extent that they concern survey methods other than those examined here). The attendance tracking system adopted was in fact in all respects adequate to the operating methods suggested in the aforementioned opinion";

- "the effective presence in service of public employees and the consequent effective execution of the tasks assigned to them are an essential condition for the pursuit of the objective of the good performance of the public administration. Consequently, the recurrence of the parameter prescribed by lett. e) of art. 6 of the Regulation and the consequent legitimacy of the processing of biomedical data in question [also in the light] of letter f) of art. 6 of the Regulation" (p. 21)

- as regards the violation of art. 9, par. 2 lett. b), of the Regulation "it is clear that the biometric verification system of attendance has been adopted by the ASP of Enna as it is expressly provided for as an obligation of the public employer placed at his charge by law no. n.56/2019 [...]" and "the processing in question is also necessary for the exercise of specific rights of the data controller in the field of labor law" as well as due to the cases of "absenteeism which occurred in the Chiello Hospital of Piazza Armerina, Hospital unit falling within the competence of the ASP of Enna";

- the treatment would also find its legal basis also in the art. 9, par. 2 lett. g) and art. 2 sexies of the letter code u) "duties of the national health service and of subjects operating in the health sector, as well as tasks of hygiene and safety in the workplace and safety and health of the population, civil protection, protection of life and physical safety", the main tasks, in fact, of a local health authority such as the ASP of Enna" (p. 26);

- "in preparing the system that would allow the biometric survey at the entrance gates, as required by current legislation, the Company has decided to adapt to the methods resulting from the previous indications of this Guarantor Authority, first of all by not setting up any contextual survey system audiovisual at the gates. This Company understands and shares the concerns that this Guarantor Authority has expressed in its opinion on the draft regulation implementing the. 56/2019" but "does not agree with the consideration expressed therein, according to which the incompatibility of the provisions pursuant to art. 2 of law no. 56 would not be remediable with the adoption of particular implementation methods of the obligation enshrined therein, since it would reside 'in the an earlier than in the quomodo of the treatment'";

- “In the face of the right to freedom constituted by the protection of personal data (and in particular of biometric data) guaranteed by national and Community legislation, there are multiple public interests which are not subordinate but equally ordered with respect to it. The assessment of these public interests and the choice to protect them through the imposition of a generalized obligation is the responsibility of the ordinary national legislator, also because the Regulation itself expresses itself in these terms. The assessment of proportionality of the treatment, therefore, must move precisely to the content and methods of the treatment itself, without, however, forgetting that the same article 2 of the law 56/2019 refers to this principle as a guiding criterion for the application of the obligation of law” (pp. 30 and 31);

- "in any case, it is believed that the exemption from the excusable error that the jurisprudence recognizes in application of art. 3 l.689\1981 [...]" as "on the one hand the legislator who introduced the generalized obligation to survey attendance through the collection of biometric data. […] On the other hand, the conduct of this same Guarantor Authority which: before the introduction of the G.D.P.R. has expressly allowed public entities performing the same functions as this Company and for purposes similar to those pursued by it to introduce a generalized attendance detection system by verifying biometric data, after the introduction of the G.D.P.R. has not - as far as it appears - ordered sanctions or prohibitions against these same entities for the same reasons now being disputed [...]";

- "the administration has requested and obtained from the legal representative of the contractor (doc.1) before proceeding with the installation of the system in question and which certifies, under the criminal and personal responsibility of the declared compliance of the system itself with the law and to the opinion of this Authority”;

- it was also clarified that "the operation of the system is currently suspended as a result of the disputes by the Guarantor".

3. Outcome of the preliminary investigation.

The personal data protection regulations provide that the employer can process personal data, also relating to particular categories of data (see art. 9, paragraph 1 of the Regulation), of employees if the processing is necessary, in general , for the management of the employment relationship and to fulfill specific obligations or tasks established by laws, community legislation, regulations or collective agreements (articles 6, paragraph 1, letter c), 9, parr. 2, lit. b), and 4, and 88 of the Regulation).

Furthermore, the treatment is lawful when it is "necessary for the execution of a task of public interest or connected to the exercise of public powers vested in the data controller" or, when "necessary for reasons of significant public interest on the

basis of Union or Member State law, which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to protect the fundamental rights and interests of the data subject" (Articles 6, paragraph 1, letter e), 2 and 3, as well as 9, paragraph 2, lit. g,) of the Regulation and 2-ter and 2-sexies of the Code).

The national legislator has defined the public interest for the processing "carried out by subjects who perform tasks of public interest or connected to the exercise of public powers" as "significant" in the matters indicated, albeit not exhaustively, by art. 2-sexies of the Code, establishing that the related treatments "are permitted if they are provided for [...] by provisions of the law or, in the cases provided for by law, regulations that specify the types of data that can be processed, the operations that can be performed and the reason of significant public interest, as well as the appropriate and specific measures to protect the fundamental rights and interests of the data subject".

As known, the definition of biometric data identifies them as "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 data fingerprints" (art. 4, point 14), of the Regulation) and are included among the "particular" categories of personal data (art. 9 of the Regulation) due to their delicacy, deriving from the close and stable relationship with the individual and his identity.

In this framework, the processing of biometric data (as a rule prohibited) is allowed if one of the conditions indicated in art. 9, par. 2 of the Regulation and, in the workplace, only when it is "necessary to fulfill the obligations and exercise the specific rights of the data controller or of the data subject in the field of labor law and social security and social protection, 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, lett. b), of the Regulation; v. as well, art. 88, par. 1 and cons. 51-53 of the Regulation).

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 was implemented, in national law, with art. 2-septies (Guarantee measures for the processing of genetic, biometric and health-related data) of the Code (as amended by Legislative Decree No. 101 of 10 August 2018 to adapt national legislation to the provisions of the Regulation). 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).

3.1. The applicability of the data protection regulatory framework to the Company's processing of biometric data.

It should first be noted that the processing of personal data consists of "any operation or set of operations, performed with or without the aid of automated processes and applied to personal data or sets of personal data, such as the collection, registration, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, diffusion or any other form of making available, comparison or interconnection, limitation , cancellation or destruction" (art. 4, point 2), of the Regulation).

Although the Company admits that "when the employee's identity is verified at the access gates, there is actually a processing of biometric personal data", the same believes that "this particular processing falls outside the scope of the legislation of the Community Regulation, as well as, consequently, from the competence of this Guarantor Authority", due to the fact that "the processing is carried out directly and personally by the interested party and therefore not subject to the application of the principles of lawfulness and correctness sanctioned by the articles 5-6-9 of the Regulation" (cf. note of the XX, pp. 6 and 7).

On the basis of the elements reported above, it must instead be considered that, contrary to what is claimed by the Company, the operations described above in any case give rise to the processing of biometric data by the Company itself, subject to the application of the regulatory framework on the protection of personal data.

Indeed, in the case under examination the Company - even though it does not keep the biometric data of the interested parties in a centralized database, but only on portable devices equipped with adequate cryptographic capabilities (badges with smart card functionality), entrusted to the direct and exclusive availability of each interested party - still processes biometric data which, as confirmed by the Company, "are found (albeit for very few moments) within" systems used by the employer for detecting attendance and for the related purposes of managing the relationship contract with its employees. This, both in the

registration phase (so-called enrollment) with the acquisition of the biometric characteristics (fingerprints) of the interested party (see also points 6.1 and 6.2 of attachment A to the provision of the Guarantor of 12 November 2014, n. 513) , both in the biometric recognition phase, when detecting attendance (see also point 6.3 of attachment A to the aforementioned provision). These treatments are, in fact, functional to allow the collection of entry and exit data of employees for the purpose of certifying compliance with working hours and for the related accounting, purposes which, in general, in the context of the public service , is provided for by a regulatory framework stratified over time (see for example, art. 22, paragraph 3 of law 23.12.1994, n. 724; art. 3 of law 24.12.2007, n. 244; art. 7 of Presidential Decree 1.02.1986, n. 13), since they cannot in any way be assimilated to those performed by the interested party to access their own mobile device "for the exercise of activities of an exclusively personal or domestic nature" (Article 2, paragraph 2, letter c), and cons. no. 18 of the Regulation).

In particular, during the registration phase, the Company acquires, through a special reader, the fingerprint of the interested party, in order to create a biometric model (i.e. a synthetic IT description of the biometric characteristic obtained by extracting from the biometric sample only the elements salient features) which is memorized, in a secure way, within the badge given to the interested party.

In the subsequent phases of biometric recognition of the interested party, the Company verifies the identity of the same by comparing the reference biometric model, stored inside the badge, and the biometric model obtained from the fingerprint presented at the time of presence detection. If the comparison operation is successful, the identity of the interested party can be considered verified and the employee's serial number is transmitted to the attendance management system together with other information (such as the date and time of stamping).

The conservation of biometric data, with secure methods on badges with smart card functionality that the administration entrusts to the exclusive availability of each interested party, responds to a design choice of the owner who, when determining the means of treatment, adopts this measure technical and organizational in implementation of the principle of minimization of the data being processed (see articles 5, paragraph 1, letter c), 24 and 25 of the Regulation), remaining however, in any case, the preliminary verification in order upon occurrence of the conditions of lawfulness to process the biometric data of employees (Article 9 of the Regulation). In fact, it is noted that, even in the previous regulatory framework, this method of storing biometric data had been expressly indicated by the Guarantor among the technical measures and expedients which, always in the presence of the conditions of lawfulness of the processing (at the time, notification and request of preliminary verification to the

Guarantor, except for the occurrence of specific cases of exemption, see paragraph 4, provision of 12 November 2014, n. 513), the owner had to adopt to guarantee the proportionality and security of the processing.

For these reasons, the adoption of this measure does not exclude, indeed it confirms, the application of the regulations on the protection of personal data to the treatments in question, as also proven by the fact that the Company has deemed it necessary to fulfill the obligation to provide interested parties with information, in the imminence of the activation of the new attendance recording system.

3.2. The correctness and transparency of the treatment: the information to the interested parties.

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

Although the Company has ensured, at first, that "all employees have been provided with the information pursuant to art. 13 of the Regulation" (see note of the XX, cit.), however the same sent the documentation with which it believes it has fulfilled the aforementioned obligation only subsequently, at the request of the Office, attached to the defense briefs (see attachment n. XX, note XX, cit.).

From an examination of this documentation, it emerges that the Company has certainly warned the staff and informed the trade union organizations of the organizational choice made, issuing for this purpose certain notes and documents that contain generic references, none of which, however, contain all the information required by the Regulation to ensure correct and transparent treatment (Article 13 of the Regulation).

Again from the point of view of correctness and transparency, it should also be noted that, in these notes and documents, the treatment is presented as fully compliant with the regulatory framework on data protection and with the indications provided by the Guarantor.

In particular, it is noted that the note addressed to all personnel, dated XX (attachment no. XX, note of XX, in files), "supplemented by the instructions posted near the detectors", merely indicates that "in application of the art. 2 of the law n. 56 of 19.6.2019 with effect from 4 November 2019 the new attendance detection system will come into operation through the use of the biometric sensor" [... this] in full compliance with current legislation on personal data, given that, such data , remain memorized only on the personal card, held only by the employee". Furthermore, in another document, called "Information on

biometric identity detection systems", it is declared that the system "is consistent with the Opinion on a draft decree of the President of the Council of Ministers concerning the regulation of implementation of the provision referred to in article 2 of the law of 19 June 2019, n. 56, containing "Interventions for the concreteness of public administration actions and the prevention of absenteeism" - 19 September 2019 because the fingerprint is encrypted and stored only on the card that remains in the employee's possession".

For these reasons, the processing appears to have been carried out in violation of the principles of lawfulness, transparency and correctness (Article 5, paragraph 1, letter a), of the Regulation) as the information documents, indicated above, do not fully represent the processing carried out, also envisaging it as compliant with the regulatory framework on data protection.

3.3. The absence of a legal basis for the processing of biometric data for attendance tracking purposes.

In the light of the elements acquired and the declarations made during the preliminary investigation, it emerged that in the month of XX (more specifically, as per the documentation in the records, starting from the XX) the Company activated a system for detecting attendance which involves the processing of employee biometric data.

The reasons that would have made the introduction of the system necessary would be linked to the "significant complexity in the management of employees" due to the number of employees ("over 2000") and the vastness of the territorial area in which the hospitals and outpatient clinics in which they provide services ("located in 22 Municipalities"); the choice would also have taken place "in the light of the provisions of law no. 56/2019". From the documentation in the file and from what was reaffirmed in the defense briefs, it emerges that the administration, in carrying out the processing, considered that the consent of the interested parties constitutes a suitable condition for the lawfulness of the processing (see Document relating to the Impact Assessment, attached to the note of the XX, cit.).

In any case, the Company proceeded to suspend the treatment following the disputes of the Guarantor: as shown by the documents, the competent management was asked to contact the company providing the service for the restoration of the "previous method of use" of the attendance detection, by deactivating the biometric recognition function (see note XX, prot. XX, annex n. XX, in deeds).

During the investigation, the Company represented that it had adapted "to the methods resulting from the previous indications of this Guarantor Authority", mentioning, among other things, the "provision of 15 September 2016 n. 357 [with which the Guarantor] expressed a positive opinion with reference to the preliminary request [of a hospital ...] for the installation of the

system for reading biometric data (fingerprints) for detecting the presence of employees on duty" (see p. 16, note dated February 17th cit.).

To this proposed in the premise that only some of the cases referred to by the Company have been submitted to the Guarantor with requests for preliminary checks, prior to the entry into force of the Regulation, it appears necessary to reconstruct the system of legal bases for the processing of biometric data for which is now provided for enhanced protection compared to the previous regulatory framework (directive n. 95/46, law n. 675/1996 and Code).

In the previous system, biometric data were not considered "sensitive", yet in consideration of their close and stable relationship with the individual and his identity, public or private data controllers could start processing, except for specific cases of exemption, subject to notification and only after submitting the treatment to the preliminary verification of the Guarantor, as conditions of lawfulness of the treatment before the start of the same (articles 17 and 37, paragraph 1, letter a) of the Code, in the text prior to the amendments of the legislative decree n. 101/2018; see Prescriptive general provision on the subject of biometrics, 12 November 2014, n. 513, doc. web no. 3556992, point 4); provision 23 November 2006, no. 53, doc. web no. 1364099 and provision 14 June 2007, XX 23, doc. web no. 1417809; as well as provisions of 22 October 2015, n. 552, doc. web no. 4430740 and 17 March 2016, n. 129, doc. web no. 4948405; more recently, these principles have been confirmed with the provision no. 249 of 24 May 2017, doc. web no. 6531525).

In this delicate area, since 2007 the Guarantor has highlighted that the principles of data protection require that other - less invasive - systems, devices and security measures be considered in advance, which can ensure the reliable verification of attendance, without resorting to the processing of biometric data (see previously, Guidelines on the processing of personal data of workers for the purpose of managing the employment relationship, respectively, employed by private employers and in the public sector provision 23 November 2006, n. 53, web doc. n. 1364099 and provision 14 June 2007, n. 23, web doc. n. 1417809). These principles are also confirmed at international level and in the positions taken by other supervisory authorities (see Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the employment context, par. 18; see also Working Party "Article 29", Opinion 2/2017 on data processing in the workplace, WP 249, paragraph 5; CNIL, deliberation 10.1.2019 https://www.cnil.fr/fr/biometrie-sur-les-lieux-de-travail-publication-dun-reglement-type and the FAQ published on 28 March 2019 “Question-réponses sur le règlement type biométrie as well as the previous guidelines “Travail & données personnells”).

In this framework, with regard to some cases of generalized use of biometric systems in the workplace, in the face of generic prevention needs regarding the possible distorted use of commonly used attendance detection tools (such as badges), the Guarantor assessed the relative treatment as disproportionate (cf., Provv.ti 30 May 2013 nos. 261 and 262 and 1 August 2013, no. 384, web doc. nos. 2502951, 2503101 and 2578547 in respect of some schools; but also January 31, 2013, no. 38, web doc. no. 2304669 against a Municipality; see also provision no. 249 of May 24, 2017, web doc. no. 6531525, concerning the multi-service card of the Ministry defense), admitting it, however, in limited hypotheses and in the presence of objective and documented needs that make the adoption of such systems indispensable, taking into account the specificity of the concrete case, the socio-economic context of reference and the characteristics of the technology used ata (see, for example, provision 15 September 2016 no. 357, doc. web no. 5505689, expressly mentioned by the Company in the defense briefs).

The strengthening of the protection of biometric data provided for in the Regulation and in the Code, as amended by Legislative Decree no. 101/2018, through the inclusion of the same in the categories of particular data, like data on health and genetics, among those assisted by a higher level of guarantees (Article 9, paragraph 2 and paragraph 4, of the Regulation), concerned primarily the legal conditions that make the processing of these categories of data lawful, even before the technical aspects and security measures.

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 involve 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), or within the scope of application of art. 9, par. 2, lit. g) of the Regulation, relating to the processing "necessary for reasons of significant public interest on the basis of Union or Member State law, which must be proportionate to the purpose pursued, respect the essence of the right to data protection and provide for appropriate measures and specifications to protect the fundamental rights and interests of the data subject".

In the first case, similar to the present case, the processing of biometric data will be permitted only "to the extent that it is authorized by Union or Member State law [...] in the presence of appropriate guarantees for the fundamental rights and interests of the 'interested party' (Article 9, paragraph 2, letter b), and conss. nos. 51-53 of the Regulation),

In this framework, in order for a specific treatment involving biometric data to be lawfully initiated, it must find its basis in a regulatory provision that has the characteristics required by data protection regulations, also in terms of proportionality of the

intervention regulatory with respect to the purposes to be pursued. This is because the legal basis of the processing, in order to be considered a valid condition of lawfulness of the processing, must, among other things, "pursue an objective of public interest and [be] proportionate to the legitimate objective pursued" (Article 6, paragraph 3, letter b), of the Regulation).

The art. 2 of the law of 19 June 2019, n. 56, containing "Interventions for the concreteness of the actions of the public administrations and the prevention of absenteeism", invoked by the Company, established that "for the purposes of verifying compliance with working hours", the public administrations - identified in pursuant to art. 1, paragraph 2 of Legislative Decree no. 165/2001, with the exception of "personnel under public law" (cf. art. 3, paragraph 2, legislative decree n. 165/2001), and those subject to the agile work discipline referred to in article 18 of the law 22 May 2017, n. 81- "introduce biometric identification and video surveillance systems to replace the various automatic detection systems currently in use" but also provides that the "implementation methods" of the law - in compliance with art. 9 of the Regulation and the guarantee measures defined by the Guarantor pursuant to art. 2-septies - are identified with the d.P.C.M., on the proposal of the Minister of the public function, subject to agreement with the unified conference (state, regions and local autonomies) and "subject to the opinion of the Guarantor pursuant to art. 154 of the Code on the methods of processing biometric data".

As known, the regulatory process, essential to integrate the system of legal bases of the processing required by the Regulation and the Code with regard to biometric data, has not been concluded - since the implementing regulation has not been adopted, which should have contained specific guarantees to circumscribe and specify the scope of the rule as well as regulate the main characteristics and methods of processing - and, lastly, art. 1, paragraph 958 of the law of 30 December 2020, n. 178 (so-called 2021 Budget Law) repealed paragraphs 1 to 4 of article 2 of the law of 19 June 2019.

In addition, the provisions with which the Guarantor expressed the due opinion on the outline of the bill and, subsequently, on the outline of the regulation (see, provision no. 464, 11 October 2018, web doc. no. 9051774 and provision n. 167 of 19 September 2019, web doc. n. 9147290), are, however, largely already known to the Company, for having expressly mentioned them in the information documents issued to staff and trade union organizations, before undertake the treatment (see annex n. XX, note of XX).

At present, therefore, there is no suitable legal basis that can satisfy the requirements of the Regulation and the Code to legitimize public administrations to implement the processing of biometric data for the purpose of detecting employee attendance pursuant to art. 9, par. 2, lit. b) of the Regulation.

The foregoing considerations also apply if it is believed that the purpose pursued by the administration, through the described treatment, is not only that connected to the management of the employment relationship but also that of increasing the efficiency of the public administration and pursuing the improvement of services , through the effective presence in service of the human resources assigned to public offices (art. 97 of the Constitution), bringing it back, as proposed by the Company, to the scope of processing necessary for "reasons of significant public interest". As known, in the margin of flexibility granted to the national legislator, the relevance of the public interest has been further declined in the context of art. 2-sexies which specified the conditions, required by art. 9, par. 1, lit. g), of the Regulation, delimiting the conditions of legitimacy of the processing, when they are necessary for reasons of significant public interest, to the existence of a regulatory provision which must specify, in addition to the reason of significant public interest, among other things, the types of data, the operations that can be performed, the appropriate measures to protect the rights of the interested parties. At present, these elements have not been identified by any regulatory provision consistent with the specific case of application identified by the Company in its defense writings.

Nor can the lack of legal basis, regarding the processing of biometric data, be overcome by the consent of the employees given that, as moreover recently reiterated by the Guarantor (most recently, provision n. 35 of 13 February 2020, web doc. n 9285411) does not normally constitute a valid prerequisite for lawfulness for the processing of personal data in the workplace, regardless of the public or private nature of the employer (cons. no. 43; art. 4, point 11), and art. 7, par. 3 and 4, of the Regulation; see, the consolidated approach at European level, "Article 29" Working Party, Opinion 2/2017 on data processing in the workplace, WP 249, p. 7 and 26 and Guidelines on consent pursuant to EU Regulation 2016/679- WP 259- of 4 May 2020).

Finally, contrary to what is claimed by the Company, the treatment in question cannot be lawfully carried out by invoking the legitimate interest of the data controller, since, not being indicated in art. 9, par. 2, of the Regulation, the same cannot constitute a suitable derogation from the general prohibition of processing particular categories of personal data, nor, moreover, can it be applied "to the processing of data carried out by public authorities" (see Article 6, paragraph 1, letter f), of the Regulation).

For these reasons, it is believed that since 4 November 2019 the Company has processed the biometric data of employees for the purpose of recording attendance in the absence of an appropriate legal basis, in violation of articles 5, par. 1, lit. a), 6 and 9

of the Regulation.

4. Conclusions.

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

The processing of biometric data of Company employees, which occurred in violation of the regulations on the processing of personal data, was undertaken, in November 2019, in full force of the provisions of the Regulation and of the Code, as amended by Legislative Decree 101/2018. For these reasons, for the purpose of determining the regulatory framework applicable in terms of time (Article 1, paragraph 2, of Law No. 689 of 24 November 1981), these constitute the provisions in force at the time of the committed violation.

The preliminary assessments of the Office are therefore confirmed and the unlawfulness of the processing of personal data carried out by the Company is noted, as the processing of the biometric data of the interested parties took place in violation of the general principles of processing and in the absence of a suitable legal basis, in violation of articles 5, par. 1, lit. a), 6 and 9 of the Regulation.

The violation of the aforementioned provisions renders the administrative sanction applicable pursuant to articles 58, par. 2, lit. i), and 83, par. 5, of the same Regulation as also referred to by art. 166, paragraph 2, of the Code.

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

Although from 23 January 2020 the Company has given instructions to deactivate the biometric recognition function when registering attendance, it does not appear in the documents that the fingerprint data, stored in the form of a biometric model inside the badges delivered to the personnel, have been cancelled. For these reasons, the treatment is still, albeit partially, in progress.

In this context, due to the unlawfulness of the processing carried out, it is considered necessary to have, pursuant to art. 58, par. 2, lit. d), of the Regulation - which provides that the Guarantor has the corrective powers to "order the data controller or the data processor to bring the data into compliance with the provisions of this regulation, if necessary, in a specific way and

within a specific term ” – the deletion of personal data (biometric models) of employees currently stored in the badges used by them, within sixty days of notification of this provision.

Pursuant to art. 157 of the Code, the Company will also have to provide to communicate to this Authority the initiatives it intends to take to ensure the termination of the treatment within thirty days of notification of this provision.

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

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

In this regard, taking into account the art. 83, par. 3, of the Regulation, in the present case - also considering the reference contained in art. 166, paragraph 2, of the Code – the violation of the aforementioned provisions is subject to the application of the same pecuniary administrative sanction provided for by art. 83, par. 5, of the Regulation.

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

It should first be noted that the Company's conduct cannot be considered as the result of an "excusable error" (cf., Civil Cassation section II - 05/17/2018, n. 12110 "The error of law on the lawfulness of the conduct can detect in terms of exclusion of administrative liability [...], only when it proves unavoidable, it being necessary for this purpose, on the one hand, that there are positive elements, extraneous to the author of the infringement, which are capable of generating in him the conviction of the legitimacy of his conduct and, on the other hand, that the author of the infringement has done everything possible to observe the law, so that no reproach can be leveled against him, not even in terms of omissive negligence, burdening the author of the infringement 'burden of proof of the existence of the aforementioned elements, necessary to be able to believe your good faith"), given that, as also known to the Company itself, the incompleteness of the legal framework relating to the processing of data bi metrics for the purpose of detecting attendance in the public sector had been detected by the Guarantor

both with the aforementioned opinions on regulatory acts and in the context of a hearing of the President of the Authority on the occasion of the hearings at the Joint Commissions I (Constitutional Affairs) and XI (Work) of the Chamber of Deputies on 6 February 2019 (doc. web no. 9080870). These elements therefore make it possible to exclude that, in the present case, an "error of law on the lawfulness of the conduct" may occur for the purpose of excluding administrative liability.

For the purposes of applying the sanction, the particular delicacy of the unlawfully processed personal data and the high number of data subjects involved (all Company employees, i.e. over 2,000 data subjects) were considered.

On the other hand, it was considered that the Company promptly suspended the treatment relating to the biometric recognition of the interested parties and that there are no previous violations committed by the data controller or previous provisions pursuant to art. 58 of the Regulation.

Based on the aforementioned elements, evaluated as a whole, it is decided to determine the amount of the pecuniary sanction, in the amount of 30,000 (thirty thousand) euros for the violation of articles 5, par. 1, lit. a), 6 and 9 of the Regulation.

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

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

ALL THIS CONSIDERING THE GUARANTOR

the unlawfulness of the treatment carried out by the Provincial Health Authority of Enna has been detected for violation of articles 5, par. 1, lit. a), 6 and 9 of the Regulation, in the terms referred to in the justification, orders pursuant to art. 58, par. 2, lit. d), of the Regulation, the cancellation of personal data (biometric models) of employees currently stored in the badges used by them, within sixty days of notification of this provision and has to communicate, pursuant to art. 157 of the Code, within thirty days from the date of receipt of this provision, the initiatives it intends to undertake to ensure the termination of the treatment. Failure to respond to a request is punished with an administrative sanction, pursuant to the combined provisions of articles 83, par. 5 of the Regulation and 166 of the Code.

ORDER

to the Provincial Health Authority of Enna in the person of its pro-tempore legal representative, with registered office in Viale A.

Diaz, 7, 94100, Enna, Tax Code 01151150867 pursuant to articles 58, par. 2, lit. i), and 83, par. 5, of the Regulation and 166, paragraph 2, of the Code, to pay the sum of 30,000.00 (thirty thousand) euros as an administrative fine for the violations indicated in the justification; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, an amount equal to half of the fine imposed;

ENJOYS

to the same Company to pay the sum of 30,000.00 (thirty thousand) euros, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the law no. 689/1981;

HAS

the publication of this provision on the Guarantor's website pursuant to art. 166, paragraph 7, of the Code;

the annotation of this provision in the internal register of the Authority, provided for by art. 57, par. 1, lit. u), of the Regulation, of the violations and of the measures adopted in accordance with art. 58, par. 2, of the Regulation.

Pursuant to art. 78 of the Regulation, of the articles 152 of the Code and 10 of Legislative Decree 1 September 2011, n. 150, against this provision it is possible to lodge an appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the appellant resides abroad.

Rome, 14 January 2021

PRESIDENT

Station

THE SPEAKER

Zest

THE SECRETARY GENERAL

Matthew