[doc. web no. 9852776]

Injunction order against the Municipality of Vicchio - 15 December 2022

Register of measures

no. 422 of 15 December 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, concerning the protection of natural persons with regard to the processing of personal data, as well as the free movement of such data and which repeals 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 individuals 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");

HAVING REGARD to the documentation in the deeds;

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

SPEAKER the lawyer Guido Scorza;

WHEREAS

1. Premise.

Following a specific report, an investigation was launched with reference to the processing of personal data of employees

carried out by the Municipality of Vicchio through a system used for the purpose of recording attendance which allowed the processing of biometric data.

In fact, during the investigation it emerged that the Municipality had installed the aforementioned system "in order to verify compliance with the working hours" by the employees employed at the municipal offices.

2. The preliminary investigation.

In response to the Office's requests for information, the Municipality, with a note of the XX (prot. n.XX), declared that:

“on the XX date, in compliance with the provisions of the provisions of Law no. 56 of 2019, so-called Concreteness Law, the Municipality, in order to verify compliance with working hours, has introduced biometric verification systems for the identity of employees and, precisely, has installed two attendance detection devices, supplied by the company Halley Informatica, located at the entrance to the town hall and at the municipal construction site”;

"the operation of biometric recognition systems was structured as follows:1) The "registration" (enrollment) phase: the reader of the terminal acquires the fingerprint and processes it according to an irreversible mathematical algorithm until obtaining a mathematical model (called template) which, associated with the person's identification code, becomes the basis for subsequent comparisons or checks; 2) The "verification" phase (matching): when the employee places his finger on the reader, the characteristics of the fingerprint are acquired, digitized, processed and compressed in the same way as in the registration phase until to obtain an analogous mathematical model. The comparison between the archived model (template acquired during registration) relating to the reference code and the result of the reading determines the result of the verification, based on the deviation. In this correlation, the mathematical algorithm is "one-way". It converts the fingerprint into x/y coordinates after which the algorithm converts these point coordinates into numerical strings (Bytes) which are stored in a model to be used for subsequent comparisons. Therefore, only the reference numbers of the x/y coordinates of the points are stored in the template and not the actual biometric characteristic. This mechanism makes it impossible to trace the imprint itself from the template, thus making the identity of the registered subjects secure in terms of privacy";

"the biometric data was processed and stored in the form of a biometric model on a badge held by the individual concerned to allow subsequent comparison operations (operations that took place with the same guarantees provided for the enrollment phase)";

"the Municipality has favored the conservation of biometric models only in devices exclusively available to the user, avoiding

their centralized archiving in databases accessible on networks, including local ones";

"in compliance with the provisions contained in the Finance Law for 2021 and, precisely, with the repeal of the provisions that allowed the introduction of biometric detection systems in the public sphere, on the XX date it deactivated these systems and reintroduced the badge, as a recording the attendance of employees on duty. The Municipality has therefore processed the personal biometric data of the employees for the period XX - XX, adopting, in that context, all the security measures for the best protection and protection of personal data, so as to privilege, in view of the privacy principles , the storage of data on devices in the exclusive availability of the interested parties".

With a note of the XX, the Office, on the basis of the elements acquired, notified the Municipality, 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 aforementioned data controller 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 the law n. 689 of 24 November 1981).

With the note mentioned above, the Office found that the Municipality had processed the biometric personal data of its employees for the purpose of detecting attendance in violation of the principle of "lawfulness, correctness and transparency" and in the absence of a suitable prerequisite of lawfulness, in violation of articles 5, par. 1, lit. a), 6, para. 1, lit. c) and 9 par. 2, lit. b), and par. 4, of the Regulation.

With a note of the XX, the Municipality sent its memorandums specifying, among other things, that:

“art. 2 of the law n. 56 of 2019, given its formulation, imposed the obligation on public administrations to replace the previous automatic attendance detection systems with "biometric identity verification systems in compliance with the principles of proportionality, non-excess and gradualness sanctioned by art . 5 par. 1 lit. c) of the Regulation (EU)";

“with provision of 12 November 2014, n. 513, entitled "General prescriptive provision on the subject of biometrics" the Guarantor for the Protection of Personal Data defined "a unitary framework of measures and expedients of a technical, organizational and procedural nature to increase the security levels of biometric processing and to bring them into line with current regulation of the protection of personal data” (see Introduction to Annex A) provision of 12.11.2014, n. 513 GDPR)”;

"it is worth noting that the opinion issued by the Guarantor on the Prime Ministerial Decree pursuant to art. 2 of Law 56/2019, indicates the opportunity to integrate the regulatory text with the provisions of provision no. 513/2014 referred to above in order

to fulfill the regulatory obligation established by art. 2 of Law 56/2019 [...]";

“the attendance tracking system adopted by the Municipality included a so-called registration phase. enrollment within which the reader of the terminal read the fingerprint and processed it, through an irreversible mathematical algorithm, in an encrypted mathematical model constituting the basis for subsequent comparisons and checks; in the subsequent verification phase, so-called Matching, the characteristics of the fingerprint were acquired, digitized and processed in the same way as in the registration phase until the same mathematical model was obtained. The comparison between the archived model relating to the reference code and the result of the reading determined the result of the verification. The mathematical algorithm used did not allow memorizing the somatic characteristics of the biometric data. Furthermore, the system as implemented did not allow to trace the mathematical model generated by the fingerprint";

“as indicated in the information sent to the employees of the Municipality in the XX, after registration, the template is memorized in order to be later compared, as explained above. In our case, the template is not stored directly in the memory of the reader device, but on a badge to be given to the employee who is personally responsible for keeping it. The data that are archived are the following: a) The user code: it is a simple reference code; b) The template model: this is a pure number that is memorized on the badge supplied to the employee. The comparisons between the memorized one and the one generated at the time of registration are always performed locally without leaving them then memorized on the terminal. This method further guarantees the employee on the confidentiality of the data, since the template is stored only on the badge provided. c) The list of events: date, time, user code, terminal address and any justification code. These are the only results memorized after the checks made by the biometric reader. In practice, these data are equivalent to the classic data of any personnel attendance terminal. The biometric reader of the terminal therefore does NOT contain: a) the personal data of the employee; b) The employee's fingerprint image; c) Direct or deducible physical data of the fingerprint. The "reconstruction" of the employee's fingerprint starting from the template is not possible, not even knowing the code of the processing algorithm by definition of an irreversible mathematical algorithm";

"the Municipality, in using the presence detection system described above, [has] complied with the prescriptions dictated by the Guarantor himself with provision no. 513/2014 and of the annex A. [...and has not] engaged in conduct that is concretely offensive to the interests underlying the provisions of the EU Regulation";

“the exemption of good faith, understood as an error on the lawfulness of the fact, also applicable in terms of administrative

offense governed by law 689/1981, takes on significance in the presence of positive elements capable of generating in the perpetrator of the violation the conviction of the lawfulness of his or her actions (Court of Appeal section I - Milan, 06/05/2021, n. 369). In other words, “In terms of administrative sanctions, pursuant to law no. 689 of 1981, article 3, for violations affected by an administrative sanction, the awareness and will of the active or omissive conduct is necessary and at the same time sufficient, without the need for concrete demonstration of willful misconduct or guilt, since the law establishes a presumption of fault in relation to the prohibited fact against the person who committed it, reserving the burden of proving that he acted without fault. It follows that the exemption of good faith, also applicable to the administrative offense governed by law no. 689/1981, is recognized as a cause for the exclusion of administrative liability - like what happens for criminal liability, in the matter of contraventions - only when there are positive elements capable of generating in the perpetrator of the violation the conviction of the legitimacy of his conduct and that the offender has done everything possible to comply with the precept of the law, so that no reproach can be leveled against him (Cass. Civil section II - 02/23/2021, n. 4830)";

"Pursuant to art. 2 law n.56/2019 imposed the obligation on public administrations to replace the previous automatic attendance detection systems with "biometric identity verification systems [...] At the same time, however, in a contradictory way, the implementation decree envisaged by the second part of the same article, creating, as a result, in the recipients of the legislative precept an inevitable disorientation on the correct conduct to be assumed”;

"the Municipal Administration in order, however, to comply with the provisions of the first part of the legislative provision referred to and at the same time to respect the principles set forth in art. 5 of the EU Regulation, has adopted the biometric system for detecting attendance described above, in compliance with the provision of the Guarantor n. 513/2014 […] evaluating the biometric detection of attendance adopted as "authorized" by the Italian legal system, being prescribed by the first part of the art. 2 of Law no. 56/2019 and, also, implemented in such a way as to guarantee the fundamental rights of the interested parties; so as to be respectful of the provision of the Guarantor n. 513/2014”;

"The complex regulatory framework described above has, therefore, generated in the Administration the conviction of the legitimacy of its conduct, resulting in the Municipality not deserving of the application of a sanctioning treatment".

On the 20th date, the hearing requested by the Municipality was also held, pursuant to art. 166, paragraph 6, of the Code, on the occasion of which the same confirmed what had already been declared in the defense briefs, specifying, among other things, that:

“The Municipality of Vicchio is a small entity, with only fifty employees;

"The Municipality referred to the general provision of the Guarantor of 2014 on biometrics in order to ensure compliance with art. 5 of Regulation (EU) 2016/679, equipping itself with an attendance detection tool compliant with the provisions of the Guarantor, not going to harm the interests that art. 2 of the law 56/2019 intended to protect";

“the system was used until the twentieth century and, therefore, for only eleven days after the abrogation of art. 2 of the law 56/2019, or for a completely reasonable time to allow the Entity to restore the ordinary systems for detecting attendance";

“the biometric detection system was in any case set up with maximum security and in full respect of the rights of the interested parties, since the treatment complies with the prescriptions given by the Guarantor at the time with the aforementioned 2014 provision on biometrics. Furthermore, specific information on the processing of personal data was provided to the workers";

"all biometric data (which referred to a number of interested parties in any case not exceeding fifty, taking into account the emergency period linked to the SARS-CoV-2 pandemic) were in any case definitively cancelled".

3. Outcome of the preliminary investigation. The applicable legislation.

The personal data protection regulations provide that the employer may process the personal data of employees, also relating to particular categories (see Article 9, paragraph 1 of the Regulation), if the processing is necessary, in general, for fulfill specific obligations or tasks established by national sector regulations and, in general, for the management of the employment relationship with the interested party and to fulfill specific obligations or tasks established by law or by Union or Member State law (articles 6, paragraph 1, letter c), 9, paragraph 2, lit. b), and 4, and art. 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" (Article 6, paragraph 1, letter e), 2 and 3, and art. 9, par. 2, lit. g), of the Regulation; art. 2-ter of the Code, in the text prior to the changes made by Legislative Decree 8 October 2021, no. 139).

With specific regard to biometric data, i.e. "personal data obtained from a specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person which allow or confirm its unambiguous identification, such as the facial image or dactyloscopic data" (art. 4, paragraph 1, no. 14) of the Regulation), it should be emphasized that, as is now known, due to their delicacy - deriving from the close (and stable) relationship with the individual and his identity - they are included among the "particular" categories of personal data (Article 9 of the Regulation).

In this context, the processing of biometric data - normally prohibited - is permitted only when one of the conditions indicated in

par. 2 of the art. 9 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 the 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 3 and the interests of the data subject" (see also, art. 88, paragraph 1 , of the Regulation and cons. 51-53).

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 9, paragraph 4 of the Regulation) which, in national law, consist in "compliance with the guarantee measures established by the Guarantor", pursuant to art. 2-septies of the Code.

The employer, data controller, is, in any case, required to respect the principles of "lawfulness, correctness and transparency", "purpose limitation", "data minimization", "accuracy", as well as "integrity and confidentiality ” and “accountability” (art. 5 of the Regulation).

3.1 Processing of employee biometric data for attendance tracking purposes

The purpose of detecting employee attendance at work, functional to certifying compliance with working hours and accounting for it - which, in general, in the public sector, is envisaged by a regulatory framework that has stratified over time (see for example, art. 22, paragraph 3, of the law 12.23.1994, n. 724; art. 3 of the law 12.24.2007, n. 244; art. 7 of the Presidential Decree 02.1.1986, n. 13) - implies a processing 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 (see also art. 88, paragraph 1, Regulation).

With regard to the compatibility with the personal data protection regulations of the pursuit of this purpose through the processing of biometric data, it should be remembered that since 2007, in the previous regulatory framework which did not include these categories of data among sensitive ones, 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, declaring the illegality of the processing carried out in the working context in the face of generic needs to prevent any incorrect behavior or distorted use of commonly used attendance detection tools, such as badges (see already, Guidelines on the processing of personal data of workers for management of the employment relationship, respectively, employed by private employers and in the public sector 23

November 2006, no. 53, doc. web n.1364099 and provv. 14 June 2007, no. 23, doc. web no. 1417809; Provisions 30 May 2013 nos. 261 and 262 and 1 August 2013, n. 384, doc. web nos. 2502951, 2503101 and 2578547 against some schools; but also 31 January 2013, n. 38, doc. web n.2304669 against a Municipality; v. also the prov. no. 249 of 24 May 2017, doc. web no. 6531525, concerning the multiservice card of the Ministry of Defence).

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”).

Within the framework outlined by the Regulation, as already anticipated (see par. 3), the processing of biometric data today requires an express regulatory provision and specific guarantees for the rights of the interested parties (the processing is in fact permitted "to the extent that it is 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), of the Regulation and cons. 51-53, and "in compliance with the guarantee measures" identified by the Guarantor pursuant to art. 9, par. 4, of the Regulation and of the art. 2-septies of the Code).

The strengthening of the protection of biometric data provided for by the Regulation and by the Code, through the inclusion of the same in the special data categories and, like health and genetic data, among those assisted by a higher level of guarantees, has in fact concerned first of all the legal conditions that justify the processing of these categories of data (see provision of 14 January 2021, web doc. n.9542071, n. 16, web doc. n.9542071; see also, more generally, with regard to a different context, provision September 16, 2021, n. 317, web doc n. 9703988).

In this context, therefore, the processing of biometric data can be lawfully carried out only where it finds its basis in a regulatory provision that has the characteristics required by data protection regulations both in terms of quality of the source, necessary contents and measures appropriate and specific to protect the rights and freedoms of the interested parties, both in terms of proportionality of the regulatory intervention with respect to the purposes to be pursued (Article 6, paragraphs 2 and 3 of the Regulation). This is because, in order to be considered a valid condition for the lawfulness of the processing, national law

must, inter alia, "pursue an objective of public interest and [be] proportionate to the legitimate objective pursued" (art. 6, paragraph 3, letter b), of the Regulation).

The art. 2 of the law 19 June 2019, no. 56, containing "Interventions for the concreteness of public administration actions and the prevention of absenteeism", had envisaged a generalized replacement of automatic attendance detection systems with biometric data detection systems together with the use of video surveillance systems providing that , “for the purpose of verifying observance of working hours”, public administrations - identified pursuant to art. 1, paragraph 2, of Legislative Decree 30 March 2001, n. 165, with the exception of "staff 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, no. 81 - "introduce biometric identification and video surveillance systems to replace the various automatic detection systems currently in use".

This generic provision also established 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 of the Code - should be identified with d.P.C.M., on the proposal of the Minister for Public Administration, 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".

In exercising its advisory powers on regulatory acts (articles 36, paragraph 4 and 58, paragraph 3 of the Regulation as well as 154 of the Code), the Guarantor had, at the time, reported to the national legislator the significant critical issues of the proposed legislation highlighting, in particular, "the excess with respect to the purposes intended to be pursued, also in terms of the gradualness of the restrictive measures that can be adopted against workers" (see provision no. 464 of 11 October 2018, doc. web no. 9051774).

As reiterated by the Guarantor also subsequently, during the hearing in Parliament in relation to this regulatory intervention, respect for the principle of proportionality must, in fact, also be ensured in the context of the balancing between different public interests and fundamental rights operated by the legislative power of the member states. Also due to the close correlation between the art. 8 of the European Convention on Human Rights and articles 7 and 8 of the Charter of Fundamental Rights of the European Union, provided for by art. 52 of the Charter itself, when a legislative measure, which must in any case respond to purposes of general interest, interferes with or limits a right protected by the Community legal order, it is necessary to assess whether it respects the "essential content of rights" and represents the "measure less restrictive" to achieve the

legitimate aim that is intended to be pursued with "the least possible sacrifice of the interests involved" in compliance with the principle of proportionality (cf., hearing of the President of the Authority at Joint Commissions I and XI, Constitutional Affairs and Labour, of the Chamber of Deputies on 6 February 2019, web doc. n. 9080870).

In the light of this framework, the regulatory provisions that introduce/authorize the processing of personal data can lead to compressions of the right to the protection of personal data within the limits of what is strictly necessary (they must be "necessary" for the interest worthy of protection that one intends to pursue in presence of a "pressing social need") and must actually respond to purposes of general interest in compliance with the principle of proportionality, grading the forms of intervention and favoring those which, in allowing the effectiveness of the objectives to be pursued, determine less serious encroachments on the "private life" of the interested parties (see the abundant jurisprudence of the European Court of Human Rights, case c-524/06-Huber/Bundesrepublik Deutschkand of 16/12/2008, as well as of the Court of Justice of the European Union, Grande Chamber, 8 April 2014, Joined Cases C-293/12 and C-594/12; sentence 20 May 2003, C-465/00, C-138/01 and C-139/01, joined; sentence 9 November 2010, C-92/09 and C-93/09, joined).

As also highlighted by constitutional jurisprudence, in balancing competing values, even if of constitutional relevance, it is necessary to verify that the solution chosen by the legislator, among the abstractly possible measures, is the most appropriate for achieving the objectives and is, at the same time, the one less restrictive of rights, under penalty of the unreasonableness and disproportion of the legislative measure (see sentence of the Constitutional Court n. 20 of 23 January 2019, point n. 5).

Confirming what has already been noted during the hearings before the competent parliamentary commissions, the Guarantor therefore reiterated, also in relation to the Prime Minister's Decree scheme which should have contained the related implementing provisions, then withdrawn as a result of the Authority's findings and never adopted, which "cannot be considered in any way compliant with the proportionality canon - as declined by European and internal jurisprudence - the hypothesized systematic introduction , generalized and undifferentiated for all public administrations of biometric attendance detection systems, due to the constraints imposed by the European legal system on this point, due to the invasiveness of these forms of verification and the implications deriving from the particular nature of the data" (see opinion no. 167 of 19 September 2019, web doc. no. 9147290).

The provisions which provided for the introduction of biometric detection systems of attendance, in the public sphere, contained in paragraphs 1 to 4 of art. 2 of the law 19 June 2019, no. 56, were then repealed by l. 30 December 2020, no. 178

(so-called 2021 budget law, art. 1, paragraph 958).

For these reasons, as reaffirmed by the Authority in decisions on individual cases against other data controllers in the public sphere by adopting the consequent corrective and sanctioning measures, in the absence of proportionate legislative measures and specific guarantees for the interested parties, the processing of data biometrics for the aforementioned purpose of detecting employee attendance could not and cannot be carried out (cf., most recently, provision no. 16 of 14 January 2021, web doc. no. 9542071, cit.; see the analogous considerations with regard to the private context, provision no. 369 of 10 November 2022, to be published).

During the investigation, the Municipality pointed out that, given the failure to adopt the implementing provisions of the aforementioned law, it would have made some choices and adopted technical measures in order to comply with the data protection regulatory framework and the general prescriptive provision on the subject of biometrics (provision of 12 November 2014, n. 513 web doc n. 3556992. In this regard, the Municipality declared that "the template [... biometric was not] stored directly in the memory of the reader device, but on a badge to be delivered to the employee who remains personally responsible for conservation", further guaranteeing the employee on the confidentiality of the data, since the template is only stored on the badge supplied".

However, these circumstances are not sufficient to exclude the holder's liability in this case.

In the premise that the aforementioned general provision does not contemplate the use of biometric data for the specific purpose of detecting attendance - instead having as its object the cases of "use of devices and technologies for the collection and processing of biometric data [...] for the verification of personal identity in the context of the provision of information society services and access to computerized databases, for access control to rooms and areas, for the activation of electromechanical and electronic devices, also for personal use, or machinery, as well as for signing IT documents" (see introduction, provision no. 513 cit.) - the following is noted.

The measures adopted and described by the Municipality respond to a design choice of the owner who, when determining the means of processing, adopts the technical and organizational measures - in implementation of the principles of accountability, minimization and data protection from the design and by default (see articles 5, paragraph 1, letter c) and par. 2, 24 and 25 of the Regulation) - remaining however, in any case, necessary the preliminary verification regarding the occurrence (or not) of the conditions of lawfulness to process the biometric data of employees for the specific purpose considered (art. 9 of the

Regulation). Moreover, even in the previous regulatory framework, when biometric data were not considered, unlike today, "sensitive" data, the memorization/conservation method of biometric data concretely adopted by the data controller had been expressly indicated by the Guarantor among the measures and technical precautions to guarantee the proportionality and security of the processing but to always be put in place after verifying the existence of the conditions of lawfulness of the processing (at the time, notification and request for preliminary verification to the Guarantor, except for the occurrence of specific hypothesis of exemption, see paragraph 4, provision 12 November 2014, n. 513 web doc n. 3556992).

Nor, moreover, as highlighted in the opinion that the Guarantor has given on the aforementioned draft of d.P.C.M. (opinion known to the data controller having expressly referred to it during the investigation) "the defect that connotes the law at its root" could not be "remedied by referring compliance with the proportionality fee to the specific implementation methods of this biometric recording obligation (modulating differently, for example, the types of data used or the retention period), which could only reduce the impact on the data subject's right to data protection". On that occasion, the Guarantor also specified that "the incompatibility of this provision with the principles of proportionality, non-excess, minimization lies in fact in the an before that in the quomodo of the treatment [i.e.] in its configuration as abstractly mandatory regardless from any concrete and specific need in this sense", concluding that "the critical issues identified in relation to article 2 of law no. 56 of 2019 which [...] therefore inevitably also extend to the draft regulation called upon to implement the provision" (see, opinion no. 167 of 19 September 2019, web doc. no. 9147290, cit.).

In the light of the foregoing considerations, it is believed that the Municipality has carried out, from the XX to the XX, the processing of the biometric data of its 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, par. 2, lit. b), and par. 4, of the Regulation.

Contrary to what was held by the data controller, the conduct cannot also 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 is inevitable, it being necessary for this purpose, on the one hand, that there are positive elements, extraneous to the author of the infringement, which are suitable to generate 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, weighing on the author of the 'offence the burden of proof of the existence of the aforementioned elements, necessary to be able to believe his

good faith").

With regard to the present case, in fact, the incompleteness of the legal framework relating to the processing of biometric data for the purpose of detecting attendance in the public sector - in addition to the critical issues in terms of the proportionality of the regulatory intervention - had been noted by the Guarantor both with the aforementioned opinions on regulatory acts and on the occasion of the hearings at the Joint Commissions I (Constitutional Affairs) and XI (Labour) of the Chamber of Deputies on 6 February 2019 (web doc. n. 9080870). These circumstances and the failure to adopt implementing rules are well known to the data controller, as highlighted by the same to justify his choices from a technical point of view, with this having to exclude that, in the case in point, "the error of law on the lawfulness of the conduct" for the purpose of excluding administrative liability. Nor can the thesis according to which the Municipality acted in the belief that it was obliged to install the aforesaid system be accepted as no consequence had been envisaged for the administrations in the event of failure to activate the aforesaid attendance detection systems and as confirmed by the fact that the Municipality adopted the system in question on the XX date, well over a year after the law n. 56/2019. Finally, in this regard, it should be considered that the installation of the system took place in a period, 2020, characterized by the Sars-Cov-2 epidemiological emergency, when the widespread use of smart working as a containment measure had been established by emergency regulations of the circulation of the virus in workplaces, especially public ones, with the exception of activities which by their very nature cannot be carried out in agile mode (see, art. 87, legislative decree n. 18 of 17 March 2020 and art.1, lett. d) of the d.P.C.M. of 22 March 2020, which provided for the performance in agile mode as an "ordinary method of carrying out work in public administrations" and, subsequently, art. 2 legislative decree 30 of 13 March 2021 as well as art. 6, d.P.C.M of 2 March 2021, in relation to the fact that in public administrations "the performance of agile work in the highest possible percentage" should be ensured).

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 - the truthfulness of which may be called upon to answer pursuant to art. 168 of the Code - although worthy of consideration and indicative of the full collaboration of the data controller in order to mitigate the risks of the treatment, with respect to the situation present at the time of the start of the investigation, however they do not allow to overcome the findings notified by the Office with the deed of initiation of the proceeding and are therefore insufficient to allow the filing of the present proceeding, since none of the cases envisaged by art. 11 of the Regulation of the Guarantor n. 1/2019.

The preliminary assessments of the Office are therefore confirmed and the unlawfulness of the processing of personal data carried out as it occurred in violation of articles articles 5, 6 as well as art. 9, par. 2, lit. b) and par. 4 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 Regulation and of the art. 166, paragraph 2, of the Code.

In this context, considering that the conduct has exhausted its effects, the conditions for the adoption of corrective measures, pursuant to art. 58, par. 2, 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).

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).

In this regard, taking into account the art. 83, par. 3 of the Regulation, in the specific case the violation of the aforementioned provisions is subject to the application of the administrative fine 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.

For the purposes of applying the sanction, the particular delicacy of the personal data processed, of a biometric nature, was considered, with respect to which the regulatory framework on the protection of personal data provides for the highest level of protection; the number of interested parties involved, i.e. the fifty employees of the Municipality, as well as the period of time for which the processing lasted (from XX to XX) and the historical context of activation of the system, given the epidemiological emergency and the extensive and generalized use of smart working in public administrations.

On the other hand, it was considered that the Municipality suspended the treatment relating to the biometric recognition of the interested parties, provided adequate collaboration during the investigation by definitively canceling all the data collected and active collaboration with the Guarantor in the course of the activity preliminary investigation; lastly, the ambiguity of the

regulatory data of primary rank which may have led the Municipality itself into an excusable error. There are no previous violations committed by the data controller or previous measures pursuant to art. 58 of the Regulation.

Based on the aforementioned elements, evaluated as a whole, it is deemed necessary to determine the amount of the pecuniary sanction, in the amount of 8,000.00 (eight thousand) euros for the violation of articles 5, 6 as well as art. 9, par. 2 and par. 4 of the Regulation

Taking into account the particular nature of the personal data being processed and the related risks for data subjects in the working context, 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 by art. 16 of the Regulation of the Guarantor n. 1/2019.

Finally, it is believed 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.

ALL THAT BEING CONSIDERED, THE GUARANTOR

notes the illegality of the processing carried out by the Municipality of Vicchio for the violation of the articles 5, 6 as well as art. 9, par. 2, and par. 4, of the Regulation, in the terms referred to in the justification;

ORDER

to the Municipality of Vicchio, in the person of its pro-tempore legal representative, with registered office in Via Garibaldi n. 1, 50039 Vicchio (Florence), Tax Code no. 83002370480 - VAT number 01443650484 pursuant to articles 58, par. 2, lit. i), and 83, par. 5, of the Regulation, to pay the sum of 8,000.00 (eight 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 the term of thirty days, an amount equal to half of the fine imposed;

ENJOYS

to the Municipality of Vicchio to pay the sum of 8,000.00 (eight 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 thirty 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, 15 December 2022

PRESIDENT

station

THE SPEAKER

Zest

THE SECRETARY GENERAL

Matthew