[doc. web no. 9852800]

Injunction order against the Municipality of Borgia - 15 December 2022

Register of measures

no. 423 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 Prof. Pasquale Stanzione;

WHEREAS

1. Premise.

The Municipality of Borgia sent resolution no. XX of the XX with which, "in the presence of some complaints presented to the

competent Authorities", it deemed it necessary to proceed in its offices "definitively with the installation of biometric fingerprint detection systems", informing the Authority "at order to make the biometric detection fully operational, in its final configuration, which currently includes a detection system with stamping by means of a badge, in line with the Concreteness decree". Recourse to the aforementioned systems would have been made to "prevent some dubious conduct" and possible anomalies regarding the observance of the service hours or in any case to avoid the recurrence of episodes, moreover not explicit, which could arouse suspicions in relation to the regular certification employee attendance.

2. The preliminary investigation.

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

“the attendance detection system using fingerprints, provisionally adopted only for a few months and co-present with the traditional system using badges, was definitively decommissioned immediately after the abrogation of paragraphs 1 to 4 of art. 2 Law 56/2019, established pursuant to art. 1, paragraphs 957 and 958 of the 2021 Budget Law n. 78/2020”;

"the processing of biometric data was carried out solely for the purpose of detecting entry and exit from the workplace with a greater degree of certainty and was made appropriate by the need to prevent some dubious conduct by some employees and from the loss of the magnetic cards currently in use”;

"the personnel in various capacities providing services in the Municipality with the obligation of stamping have been informed in advance using the form attached to this note that each recipient has signed for acceptance, thereby expressing their explicit consent to the processing of personal data";

"the biometric stamping system has never been exclusive and mandatory given that the device installed also worked through the traditional badge, which is why the use of one or the other method has always fallen within the sphere of discretion of the staff";

"regarding the failure to communicate the name of the contact details of the new RDP, we regret the delay as the protocol number 2 needed to access the online procedure had been lost, the recovery of which was requested by email from the XX”;

"after receiving the [...] communication [from the Guarantor] of the XX, we found the protocol number, which [had been lost] due to a very trivial move and reorganization of the sector (Financial Area) [... and it is] was made the communication of variation of the resulting data registered in the RDP Register n. XX of the XX”.

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 has implemented the processing of 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 and in violation of Article 37 of the Regulation, relating to the failure to communicate the name and contact details of the Data Protection Officer (hereinafter "DPO").

With note of the XX, the Municipality sent its defense briefs specifying, in particular, that:

"with note prot. XX of the XX The Entity communicated the definitive discontinuation of the presence detection system by means of fingerprints, immediately after the abrogation of paragraphs 1 to 4 of art. 2 Law 56/2019, established pursuant to art. 1, paragraphs 957 and 958 of the 2021 Budget Law n. 78/2020 specifying that this system had never been exclusive and mandatory given that the installed device also worked through the traditional badge and that, although each recipient had expressed their explicit consent to the processing of personal data by signing the specific information attached to the the aforesaid note, could, however, have applied for stamping by means of a badge";

"the legal basis for the decision to adopt an attendance detection system using fingerprints on an experimental basis (in the presence and at the choice of the employee of a detection using a magnetic badge) can be traced back to art. 2 of Law 56/2019 (the so-called "Concreteness Law") which entered into force on 7 July 2019";

"in the light of the aforementioned article, this Administration considered in good faith that it was in a situation of regulatory vacatio (not attributable to it, but to the non-adoption, at national level, of the Decree referred to in Article 2 of the So-called Concreteness Law) to introduce an attendance detection system using biometric fingerprints on an experimental basis, and it is remembered - in co-presence - with a magnetic badge, deeming the use lawful, because it is based on the aforementioned article, after obtaining the explicit consent of the employees and aimed solely at put order on the time of entry and exit";

"it is also specified that, although installed, the device actually registered fingerprints and entries only in the days of the XX";

"the reader has in fact immediately manifested technical malfunctions, blockages and anomalies such as to make it impossible to proceed in any way to detect the start and/or end of the work, so much so that the reader was sent for assistance and not was more put into operation, as shown by the report of the computer technician (attached to this document), which is why the employees who carried out their activities in the presence, have equipped themselves with paper registers on which they put their signature on entry and outgoing until the installation of a new ordinary time marker functioning via magnetic badge";

"from the above it follows that there was no "invasive" processing of biometric data (as it was limited only to those employees who used it - 15 to be exact) but limited to only three days in which the device detected the attendance";

"Biometric data was kept only for the short period between the 20th and 20th centuries. The XX the device was decommissioned as, among other things, emerges from the report of the IT technician referred to above";

"with reference to attendance tracking, it is essential to specify that the biometric fingerprint could not be associated with the names of the employees but with a reference numerical code, elaborated by a mathematical algorithm, therefore a pseudonymisation aspect was used in order to protect the information and data of the employee himself";

"in relation to the stampings recorded, in the three days indicated, it is not clear from the attendance recording procedure whether they had been implemented with the biometric fingerprint or with the badge" and "there is no service provision which would impose the use of biometric detection, waiting for the Guarantor to allow its definitive use";

"the communication of the change in the name and data of the new DPO [...], an employee of the Organization with the profile of administrative instructor, classified in the Technical Area of this Municipality and appointed with Trade Union Decree n. 10 of 07.13.2020, was not carried out immediately after the appointment, as, for reasons of reorganization of the premises of the Area to which the previous DPO belonged, the "Privacy" file had been located together with other files";

"to proceed with the replacement of the DPO, that Protocol number was needed [...] provided [by the Guarantor] illo tempore in order to be able to access the online procedure which represented and represents the only channel that could be used for this specific purpose";

"not being able to proceed with the communication with other valid channels, the recovery of the protocol was requested by mail of the XX which was followed [...] communication [from the Guarantor] of the XX";

"only following the rearrangement of the wardrobes and the repositioning of the folders contained in paper boxes was it possible to access the Privacy file and the Protocol number. [...] it is evident [..., therefore,] our perfect good faith [...]";

"it appears clear that the disputed omission is attributable to an unintentional error, so much so that as soon as the protocol was retrieved [...] the resulting data variation communication was promptly made and registered in the RDP Register no. XX of the XX which was followed by the updating of the data on the Municipality's website".

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, in particular, that:

“the attendance system employed included a fingerprint reader”;

“the Municipality started an experiment that lasted only three days, as the fingerprint reader did not work properly; even in this limited period of time, the employees were still unable to register their presence using the reader due to some malfunctions”;

“the Municipality acted in total good faith, on the basis of the so-called concrete law, in the belief that the treatment was lawful, as required by a law, as the Municipality was not aware of the non-implementation of the law or of the Guarantor's guidelines on the matter";

"the good faith of the Municipality is proven by the fact that the Body spontaneously informed the Guarantor of the treatment before the start of the investigation";

Moreover, the Municipality did not oblige the employees to stamp with a fingerprint, given that it was an experiment, the participation in which was entirely optional on their part. Only n. 13 employees”;

“employee data, acquired in the so-called enrollment phase, were definitively canceled on date XX, when the system was definitively decommissioned".

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, letter 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 in the categories " details" of personal data (art. 9 of the Regulation).

In this context, the processing of biometric data (as a rule prohibited) is allowed if 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" (art. 9 paragraph 2, letter b) of the Regulation; v. as well, art. 88, par. 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", "minimization" as well as "integrity and confidentiality" of data and "accountability" (Article 5 of the Regulation).

With regard to the figure of the DPO, the legislation on data protection provides that the designation of the same is always due by a "public authority" or a "public body" (Article 37, paragraph 1, lett. a), of the Regulation).

The DPO must be equipped with the “resources necessary to perform [his] duties […]” and “may perform other tasks and functions. The data controller or the data processor ensures that these tasks and functions do not give rise to a conflict of interest" (Article 38, paragraphs 2 and 6, of the Regulation; see cons. 97 of the Regulation, where it is stated that DPOs “should be able to carry out the functions and duties assigned to them independently”).

With specific reference to the prohibition of conflicts of interest, the "Guidelines on data protection officers" (adopted by the Article 29 Working Party on 13 December 2016, in the amended version on 5 April 2017) specify that "the absence of of

interests is strictly connected to the independence obligations. Even if a DPO may perform other functions, the assignment of these additional tasks and functions is possible only on the condition that they do not give rise to conflicts of interest. This means, in particular, that a DPO cannot play, within the organization of the data controller or data processor, a role that involves defining the purposes or methods of processing personal data. This is an element to be taken into consideration on a case-by-case basis, looking at the specific organizational structure of the individual data controller or data processor" (par. 3.5, p. 21).

The data controller must publish the contact details of the data protection officer and communicate them to the supervisory authority (Article 37, paragraph 7, 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 law 23.12.1994, n. 724; art. 3 of law 24.12.2007, n. 244; art. 7 of 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, declaring the illegality of the treatments carried out in the workplace in the face of generic needs of prevention of any incorrect behavior or misuse of commonly used attendance detection tools, such as badges (see already, 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 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 for this purpose 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 which 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 data subject", 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, through their inclusion in the special data categories and, like health and genetic data, among those assisted by a higher level of guarantees, has in fact concerned above 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, provv 16 September 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 source quality, necessary content and of appropriate and specific measures 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 of 19 June 2019, n. 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 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".

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 the d.P.C.M., on the proposal of the Minister of 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 article 154 of the Code), the Guarantor had, at the time, reported to the national legislator the significant criticalities of the regulatory proposal, 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 , web doc. n. 9051774).

As reaffirmed by the Guarantor also subsequently, during the hearing in Parliament in relation to this regulatory intervention, the principle of proportionality represents a condition to which the work of 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 ECHR and the 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., on this point, hearings before 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 copious jurisprudence of the ECtHR, case c-524/06-Huber/Bundesrepublik Deutschkand of 16/12/2008; European Court of Justice, Grand Section, 8 April 2014, Joined Cases C- 293/12 and C-594/12; Court of Justice, sentence 20 May 2003 C-465/00, C-138/01 and C-139/01 (joined); Grand Section Court of Justice, 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 unreasonableness and disproportion of the legislative measure (cf. Constitutional Court n. 20 of 23 January 2019, therein, point n. 5).

Confirming what has already been noted during the hearings before the competent parliamentary commissions, therefore, the Guarantor reiterated, also in relation to the d.P.C.M. 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 attendance detection systems, in the public sphere, contained in paragraphs 1 to 4 of article 2 of law 19 June 2019, n. 56, were then repealed by l. 30 December 2020, no. 178 (so-called 2021 Budget Law, art. 1, paragraph 958).

With regard to what was declared by the Municipality regarding the initiatives taken to fully inform employees and acquire the relative consent to the processing of biometric data, it should be noted that, even before the repeal of Law no. no. 56/2019, the findings made by the Guarantor to the national legislator regarding the regulatory intervention in question, could not be overcome by any consent from the employees concerned. In general terms, the worker's consent 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 (recital 43 of the Regulation), this in the light of the asymmetry between the respective parts of the employment relationship and the consequent, possible, need to ascertain, from time to time and concretely, the effective freedom of the employee's expression of will (see, among others, provision n. 16 of 14 January 2021, web doc. n. 9542071; n. 35 of 13 February 2020, web doc. n. 9285411; n. 500 of 13 December 2018, web doc. n. 9068983; see also articles 6- 7 and recitals 42-43, Regulation (EU) 2016/679; see also, in a compliant sense, Article 29 Group, Guidelines on consent pursuant to EU Regulation 2016/679 - WP 259 - of 4 May 2020, specifically . para. 3.1.1.; Opinion 2/2017 on data processing in the workplace, WP 249, spec. para. 3.1.1 and 6.2)

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 data subjects, the processing of data biometrics for the aforementioned purpose of detecting employee attendance, could not and cannot be carried out (see, most recently, provision no. 16 of 14 January 2021, web doc. no. 9542071 but also the analogous considerations with regard to the private context, provision n. 369 of 10 November 2022, to be published).

In the light of the foregoing considerations, it is believed that the Municipality has carried out, albeit for a limited period, a processing of the biometric data of employees for the purpose of recording attendance in the absence of an appropriate legal basis, in violation of articles 5, 6 as well as art. 9, par. 2 and par. 4, of the Regulation.

3.2. Failure to provide the name and contact details of the Data Protection Officer

In taking note of what was declared by the Municipality regarding the errors that would not have allowed the timely communication of the contact details of the new DPO, it is reiterated that the art. 37, par. 1, lit. a) of the Regulation provides for the obligation, for each public authority or public body that processes personal data, to designate a DPO and to communicate to the Supervisory Authority the name and contact details of the same.

In order to comply with the obligation in question, the online procedure, made available by the Guarantor for the communication, change and revocation of the name of the designated DPO, represents the only channel that can be used for this specific purpose (available on the page https://servizi. gpdp.it/comunicazionerpd/s/, where the specific instructions are also given; see Guidelines on data protection officers (DPOs) adopted by the Art. 29 Group on 13 December 2016 and amended on

5 April 2017 WP243 rev. 01 and FAQs relating to the telematic procedure for the communication of DPO data https://www.gpdp.it/regolamentoue/rpd/faq, relating-to-the-procedura-telematica-per-la-comunicazione-dei-dati).

It should be noted, in more detail, that, as regards the change in the contact details of the DPO (for example, due to the appointment of a different person for that task), it must be done promptly, again through the procedure indicated above, so that the Authority, for the exercise of its duties, is always in possession of updated information and, consequently, addresses the exact "point of contact" (the maintenance of contact details that are no longer current could involve the involvement of a person who has ceased to perform his duties as DPO).

For these reasons, failure to update the contact details of the DPO, both on the website of the entity and in the related communication to the Authority, constitutes a conduct that can be punished in the same way as failure to publish/communicate (see Article 37, paragraph 7, of the Regulation, the violation of which is subject to administrative sanctions pursuant to Article 83, paragraph 4, letter a), of the same Regulation). These principles were lastly reaffirmed by this Authority in the guidance document adopted to provide clarifications to the administrations regarding the designation, position and tasks of the DPO in the public sphere (provision no. 186 of 29 April 2021, web doc. no. 9589104).

Given the above, it must be concluded that - prior to the communication of the change in the contact details of the DPO, which took place following the request for elements by the Office - the Municipality gave rise to the violation of art. 37 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 - 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 the notified findings to be overcome by the Office with the act of initiation of the procedure and are therefore insufficient to allow the filing of the present procedure, since none of the cases provided for 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 5, par. 1, lit. a), 6, 9, para. 2, lit. b), and par. 4, as well as 37, par. 7, 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. 5 of the Regulation, in this case - also considering the reference contained in art. 166, paragraph 2, of the Code – the violation of the aforementioned provisions is subject to the application of the same pecuniary administrative sanction provided for by art. 83, par. 5, of the Regulation.

The aforementioned pecuniary administrative sanction imposed, 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 nature, object and purpose of the processing involving biometric data - with respect to which the regulatory framework on the protection of personal data provides for the highest level of protection - referred to employees for attendance tracking purposes.

On the other hand, it was considered that the Municipality is a small entity, that the treatment was carried out, on an experimental basis, for a very limited period of time (particularly from the XX and the XX, given that "The XX the device is been decommissioned"), spontaneously informing the Authority and that the system in question was an alternative to the traditional presence detection by means of badges; some specific factual circumstances were also taken into account, represented by the data controller during the preliminary investigation and, in particular, that the actual use of the system for the daily verification of the presence in service "lasted only three days , as the fingerprint reader did not work properly" and would have been used

in recent days only by some interested parties, i.e. those who had decided to participate in the trial (only 13 employees). As for the violation of art. 37 of the Regulation, account was taken of the mistake that the Municipality incurred which would have resulted in the delay in communication. Furthermore, the Municipality provided adequate collaboration during the investigation and 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 deemed necessary to determine the amount of the pecuniary sanction, in the amount of 5,000.00 (five thousand) euros for the violation of articles 5, 6, par. 1, lit. a), 9, para. 2 and par. 4, as well as 37, par. 7, 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 treatment carried out by the Municipality of Borgia for the violation of the articles 5, par. 1, lit. a), 6, 9, para. 2 and par. 4, as well as 37, par. 7, of the Regulation, in the terms referred to in the justification;

ORDER

to the Municipality of Borgia, in the person of its pro-tempore legal representative, with registered office in Corso Mazzini - 88021 Borgia (CZ), Tax Code 00291270791, pursuant to articles 58, par. 2, lit. i), and 83, par. 5, of the Regulation, to pay the sum of 5,000.00 (five 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 Borgia to pay the sum of 5,000.00 (five 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

station

THE SECRETARY GENERAL

Matthew