Deliberation 2019-001 of January 10, 2019 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Wednesday October 13, 2021 NOR: CNIL1908954X devices whose purpose is to control access by biometric authentication to premises, devices and computer applications in the workplaceThe National Commission for Data Processing and Liberties, Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to the automatic processing of personal data; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), in particular its article 9, paragraphs 1, 2 and 4; Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its articles 8 and 11-I-2° (b); Considering the decree n° 2005-1309 of October 20, 2005 modified taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; After having heard Mrs. Marie-France MAZARS , commissioner, in her report, and Ms. Nacima BELKACEM, government commissioner, in her observations, Makes the following observations: new, that of establishing and publishing, in consultation with the public and private bodies representing the players concerned, standard regulations with a view to ensuring the security of personal data processing systems and governing the processing of biometric data , genetics and health . As such, the Commission may prescribe additional measures, in particular technical and organizational, for the processing of biometric data, which have become sensitive within the meaning of Article 9-1° of the General Data Protection Regulation (hereinafter GDPR). , as well as genetic and health data pursuant to 4° of the same article. biometrics to premises, devices and computer applications in the workplace. It comes following a public consultation carried out from 3 to 30 September 2018. As a result, the Commission adopts the following model regulation: Article 1 - Purpose and scope of this regulationIn accordance with the provisions of Articles 9-4° of the GDPR, 11-I-2°-b) and 8-II-9° of the amended law of 6 January 1978 relating to data processing, files and to freedoms, the purpose of this standard regulation is to set specific requirements applicable to the processing of biometric data necessary for the control by public or private employers of access to workplaces as well as to the devices and applications used in the context of missions entrusted to employees, agents, trainees or service providers (hereinafter, persons concerned). Biometric data is understood, in accordance with Article 4-14) of the GDPR, as personal data resulting from specific technical processing, relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm its unique identification, such as facial images or fingerprint data. These data are considered sensitive within the meaning of

Article 9 of the GDPR.Constitutes a template, within the meaning of this standard regulation, the result of the processing of the raw recording (photo, audio recording, etc.) of the biometric characteristic by an algorithm making it impossible to reconstruct it. The templates constitute derived biometric data and must therefore be distinguished from the data from which the biometric characteristics are derived. The standard regulations are not intended to replace the general obligations arising from the GDPR and the amended Data Protection Act, but complete or clarify some of them. Organizations implementing such processing must therefore comply with all other legal and regulatory requirements relating to the principles of data processing, the rights of individuals or the international transfer of data. Organizations must ensure that the access control processing concerned is justified with regard to Article 6 of the GDPR. Article 2 - Purposes of the processing The use of biometric devices is only authorised, within the scope of this standard regulation, for the following purposes: controlling access to the premises limitedly identified by the organization as having to be subject to a restriction of movement; the control of access to the organization's restrictively identified professional IT devices and applications. Article 3 - Justification for the use of biometric data processing The controller must demonstrate the need to use biometric data processing, indicating the reasons for which the use of other identification devices (badges, passwords , etc.) or organizational and technical protection measures do not make it possible to achieve the required level of security. This justification must: detail the specific context making a high level of protection necessary; detail the reasons justifying the use of biometrics rather than another technology; be documented by the controller. Article 4 - Personal data collected and processed Within the framework of this standard regulation, the biometric access control device may only include the following personal data: Data entered by the employer or his employees (identification data): identity: surname, first names, photograph, raw recording (photo, audio recording, etc.) of the biometric characteristic and template(s) of one or more biometric characteristics, authentication number or individual support number, life professional: internal registration number, corps or department to which they belong, rank, identity or company name of the person (natural or legal) having the status of employer; access to premises: authorized access, zones and time slots; access to work tools: equipment or applications concerned, time slots and authorized access methods. Data generated by the device (logging data): access logging to the premises: access used, timestamp of access attempts, authentication number or individual support number; logging of access to work tools: equipment or applications concerned, timestamp of access attempts, authentication number or individual support. Article 5 - Biometric data Is authorised, in a professional environment, biometric authentication based on the morphological characteristics of the persons concerned. Biometric authentication

requiring a biological sample (saliva, blood, etc.) is prohibited within the scope of these regulations. The choice of the type or types of biometrics (iris, fingerprint, hand vein network, etc.) must be justified and documented by the employer, in particular the reason for using one biometric characteristic rather than another. Article 6 - Persons authorized to process data Authorization profiles must be provided in order to manage access to data in as needed. Authorized persons can only access the data within the limits of their powers. An annual review of the authorizations must be carried out in order to ensure that the rights granted remain consistent with the persons authorized and their functions. Concerning biometric data: Only persons who are restrictively authorized by virtue of their functions can have access to biometric data. to manage the enrollment of the person concerned, to delete the templates or to ensure the maintenance of the device. They must only access these templates within the framework of their authorization on a temporary basis and for the strict needs of the aforementioned actions.Concerning the other data entered by the employer or his employees: May have access to the other personal data entered in the biometric device (identity, professional life, access to premises, equipment and applications) the persons who are exclusively authorized by reason of their functions to manage the enrollment of the person concerned, the deletion or modification of their access profile, or maintain the device. Concerning the data generated by the device:Only can have access to the data generated by the biometric device, the people who are restrictively authorized because of their functions to ensure the security of the premises, materials and applications concerned, or the security of the biometric device itself.Article 7 - Choice of procedures for holding the templateThis regulation distinguishes three types of holding biometric templates, depending on the degree of control exercised by the persons concerned over the storage medium:Type 1: templates under the control of the persons concerned are those whose only durable storage medium is held by the person himself, for example in the form of a badge or smart card; Type 2: templates under shared control are those whose durable storage medium is controlled by the employer or his servants, but which are kept in a form rendering them unusable without the use of a secret of held by the person concerned; Type 3: templates not mastered by the persons concerned are those whose durable storage medium is mastered by the employer or his employees in a usable form requiring neither a badge containing the template nor the use of a secrecy controlled by the person concerned. In the absence of special circumstances mentioned in the following paragraphs, the processing of biometric data set up by public or private employers can only use templates under the control of the persons concerned (type 1). Templates under shared control (type 2) can only be used if it is proven that the possession of a medium dedicated to the sole storage of the template (type 1) is not adapted to the architecture and the context. operation of

the device. In the same way, templates not controlled by people (type 3) can only be used if it is proven that the installation of templates under shared control (type 2) or templates under the control of the persons concerned (type 1) is not suitable given the architecture and operating context of the device and only if the security elements provided for in article 10 are supplemented by the risk analysis on the rights and freedoms of individuals provided for in Article 11. The decision to use type 2 or 3 templates must be documented in detail, justifying the choice made. Article 8 - Terms and durations of storage Raw recordings (photo, audio recording, etc.) of the biometric characteristic can only be processed for the time necessary to calculate the template(s): they cannot therefore be stored. Derived biometric data can only be kept in the form of encrypted templates that do not allow the original biometric characteristic to be recalculated. They can only be kept for the duration of the authorization of the person concerned, and must be deleted in the event of withdrawal of in the event of termination of the functions of the person concerned in the employing organization. The access logging data produced by the biometric device cannot be kept in an active database for more than six rolling months from their date of recording. However, this does not preclude their conservation in the form of intermediate archives separate from the active database, with restricted access, insofar as there are specific legislative or regulatory provisions, or even if these data would be of interest in the event of litigation. , justifying their retention for the time of the applicable prescription/foreclosure rules. Identification data, other than biometric templates, must be deleted at the latest within six months following the date of the withdrawal of authorizations or that of the cessation functions of the person concerned within or on behalf of the natural or legal person having the quality of the employer. As a reminder, this deletion does not impact the other processing operations put in place by the employer for different purposes and relating to similar data. Article 9 - Information of persons Without prejudice to its obligations relating to information and c onsultation of the staff representative bodies, the employer provides the persons concerned with the mandatory individual information provided for in Articles 12 and following of the GDPR. This information must appear in a written notice given by the data controller to each person concerned prior to the enrollment of the latter's biometric data. Article 10 - Data security The controller shall take all necessary precautions, with regard to the nature of the data and the risks that the processing poses to the persons concerned and their rights, to preserve the availability , the integrity and confidentiality of the data processed. To this end, the data controller adopts at least the following measures or measures the equivalence of which he demonstrates: Measures relating to data: partition the data during their transmission and storage ;encrypt biometric data, including templates, using a crypt algorithm graphics and state-of-the-art key management; in particular, an encryption

and key management policy must be clearly defined (change of default keys, state-of-the-art algorithms and key size, planned renewal, etc.); integrity of the data (for example, signature or hash); integrating a technical or organizational measure for detecting fraud (for example: measure for detecting false fingers); prohibiting any external access to the biometric data (for example by implementing comparison type measurements on card (match-on-card) or physical/logical security module of HSM (Hardware Security Module) type; perform access control by comparing the calculated sample and the recorded enrollment template (on an internal/remote basis or on an individual medium) without a copy of the template; prohibit the transmission of any template stored by the employer outside the system; ensure the effectiveness of the deletion of data at the end of the e conservation (physical destruction of returned cards in the presence of the person concerned or information on the means of destroying the chip in the absence of return, automated and secure deletion of data in the database, etc.); delete the biometric data in case of unauthorized access to the read-comparison terminal or to the remote server (not applicable to type 1 storage); delete any data not useful for subsequent processing at the end of life of the biometric device. Measures relating to the organization :make the people concerned responsible for the proper conditions of use of the equipment;provide an alternative emergency device or one used on an exceptional basis, without constraint or additional cost for people who do not use the biometric solution; in particular, for people who do not meet the constraints of the biometric device (enrollment or reading of biometric data impossible, disability making it difficult to use, etc.) and in anticipation of the unavailability of the biometric device (such as a malfunction of the device), a backup solution must be implemented to ensure continuity of the service offered, limited however to exceptional use; test the system according to a formal procedure, before its implementation and after any modification, in an environment dedicated and without resorting to real data. The use of biometric data of volunteers, which cannot be linked to their real profile but to profiles created for the tests for the validation of proper functioning, must be limited to what is strictly necessary. All data must be deleted no later than the end of the tests; determine the actions to be taken in the event of authentication failure (impossibility of verifying an identity, lack of authorization to enter a secure area, etc. .); strictly manage physical and logical access to devices and databases by authorized persons; in particular, a rights and access management policy must be clearly defined; it is a question of formalizing the different categories of authorized persons (users, administrators and database managers, persons in charge of data management, technical maintenance persons, etc.), their rights on the data, the way in which permissions are managed, how access to them is controlled, how secrets are managed, traces logged, how traces are managed, etc. ;specifically train administrators and persons authorized to

manage data (enrolment, processing, deletion, etc.);warn the persons concerned in the event of unauthorized access to their data;formalise, apply and publicize a backup procedure in the event of incident (providing in particular for re-enrolment). Hardware Measures: Implement measures to either alert or remove biometric data in the event of a break-in attempt on the drive or storage device. In particular, if the data is stored on a local database integrated into the biometric device, any attempt to open or pull out the reading-comparison terminal must be detected, followed by a report to the administrator of the device; reserving specific equipment for storing biometric data, or even processing data; using equipment certified to the conditions of use and in terms of security; guaranteeing the traceability of the life cycle of the equipment. Measures relating to software: reserving specific software for the use of the data; sign the software and verify its signature; keep the software up to date according to a formalized procedure; check that the modifications made by the software publishers do not promote data leakage; use detection and protection against malicious software and spyware, tested and kept up to date; limit user actions on the software; guarantee the traceability of the software life cycle; regularly check the licenses of the software used; prohibit the installation of software allowing internal observation (in the case of a badge); ensure the partitioning of the execution environment of the biometrics application. Measures relating to computer channels: securing computer channels (reserved and encrypted channels). The data controller must regularly, and at least every year, monitor the proper implementation of these measures. He must also carry out a watch allowing him to act within a reasonable time in the event of modification by the CNIL of this list of measures.Article 11 - Impact analysis relating to data protectionIn accordance with deliberation No. 2018-327 of 11 October 2018 adopting the list of types of processing operations for which a data protection impact assessment is required, the processing operations governed by this standard regulation are considered to be likely to create a high risk for the rights and freedoms of the natural persons concerned. Consequently, an impact analysis relating to data protection must be carried out by the controller prior to their implementation, whatever the type (1, 2 or 3) possession of the chosen biometric template, in accordance with Article 35 of the GDPR. The controller must therefore both comply with the provisions of this standard regulation, document er and make available to the CNIL the justifications requested therein and carry out an assessment of the risks to the rights and freedoms of individuals in order to identify them and, if necessary, to process them. The choice to use the methods of possession of the biometric template guaranteeing less control of the person, in particular of type 3, must be the subject of particularly detailed documentation. The data controller illustrates the residual risks and estimates them in terms of seriousness and likelihood. He must regularly update, at least every three years, this risk assessment as well as the

additional security measures that would result from it. This deliberation will be published in the Official Journal of the French Republic. The President I. FALQUE-PIERROTIN