Subjects: Biometrics
Occupation: Employee
Data type: Biometrics

Does management have the right to demand the collection of my biometric data?

An employee uses a magnetic key to access his workplace. The management decided to change the magnetic access control with a biometric control (iris scanner or hand geometry and fingerprints). They announced this change to the personnel.
An employee then phoned a trade union who explained that it is "completely illegal" and that the staff should "refuse to partake" and that dismissal on this ground would be "highly abusive." The employee informed his superior that he did not intend to be subjected to the collection of fingerprints. Informed of the intention of the employee, the management let it be understood that they would consider this lack of collaboration as an unacceptable violation of the employment contract. The supervisor, now worried about this situation, called upon the advisor (or person in charge) for data protection and organized a meeting with a representative of the management office to assess the situation.
At the end of the session, they admitted that the proposed data collection was not proportionate to the actual aim and it would therefore be necessary to obtain the consent of each employee. The management postponed the project and promised to study a less intrusive solution.
The data collected to allow a biometric check can be used for purposes unrelated to the stated goal. The employee was pleased that his fears had been heard.

Recommendations
The biometric data usually includes some delicate data (particularly health). When this is the case, a formal legal basis is required and the persons concerned must be clearly informed and must consent to the processing of this data. The goal must be clear, and the most adequate and less intrusive measures must be chosen. These measures must be adequately communicated. In addition to this, the employer must also consult the employees or their representatives and, in the absence of a formal legal basis, obtain their free and informed consent prior to the introduction of an automated system for the processing of personal data.

Basic principles
LIPAD 38 and 42 ; LPD 4 al. 4, 12 and 13 ; LTr 6 ; OLT3 26 ; CO 328 and 328b

Protection of privacy, protection of workers, the principle of proportionality: these measures must be necessary and the least intrusive possible.

Resources
The private bank Pictet & Cie in Geneva have been using 3D facial recognition to secure the access to its buildings since 2006. How did they overcome the fears of its 2,000 employees? Through communication. This technology does not monitor the health of an individual and violate their privacy. "The employees feared that their facial scan could affect their health, which is not the case because the machine simply films," says Jean-Pierre Therre, in charge of the security of the private bank. The database bank does not contain any photos of the employees either, but analyses the scans of their skulls according to the 40,000 reference points, and from which nothing can be drawn from :
http://www.1234economy.com/biometrie-et-reconnaissance-faciale-en-3d-comment-la-banque-privee-genevoise-pictet-a-gere-les-resistances /