Subjects: Biometrics
Occupation: Manager
Data type: Biometrics

Can I collect the biometric fingerprints of my staff?

The management wanted to avoid its employees having a magnetic key to enter the building and to clock in. They decided to implement a biometric access control. Through an internal mail, the employees were invited to give their biometric prints (hand geometry and fingerprints).
Three people were absent. When they were asked to explain their absence, they said that they had been informed that the use of such a device would be a serious breach of their privacy, and they refused to be subject to the collection of fingerprints.
The management made more precise enquiries on the measures to be observed when installing and using such a system. They contacted the consultant for the protection of corporate data or the federal commissioner / cantonal. They summoned all employees to discuss the benefits of the new system. They explained to them that they had contacted the authorities and they could ensure that the system would not be misused, and that the data would be stored securely, etc.. One of the employees did not budge: “there are easier ways to control access to the premises, such as magnetic cards ...” The management then proposed a vote by show of hands. The three recalcitrant employees demanded that the vote be held by secret ballot,
The ballots were counted: and the status quo prevailed. The management agreed that the proposed data collection was not proportionate to the aim and it was therefore necessary to obtain the consent of each employee. Given the cost and complications that would result from the presence of two parallel devices (magnetic and biometric), they postponed the project and promised to study a less intrusive one.
The data collected to allow a biometric check can be used for purposes unrelated to the stated goal. The management is encouraged to look for a creative solution that respects the privacy of the employees.

Recommendations
The biometric data usually includes some sensitive 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 /