BIOMETRICS IN THE WORK PLACE: HOW TO STAY COMPLIANT

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Delphine Daversin | May 20, 2019

Biometrics is often presented as an ergonomic and effective alternative to using too many passwords that are too difficult to remember. Biometrics authentication (or realistic authentication) can be used very conveniently by employers used as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance[1]

Biometric identifiers include, for example, fingerprint, face recognition, DNA, palm print, hand geometry, iris or voice recognition. These identifiers are permanent over time and allow to uniquely identify a natural person.

This is precisely why, in the event this data would be compromised, they present high risks and consequences for their owner's privacy.

The European Regulation for Data Protection ("**GDPR**") which came into force in 2018 as well as the Protection of Personal Information Act, Act No 4 2013 ("**PoPIA**"), soon to be enforced in South Africa, both recognize the particular character of biometric data, qualifying them respectively as "sensitive" or "special", like data on health, political opinions or religious beliefs. The processing of these sensitive or special data is in principle forbidden except in certain cases that are exhaustively listed.[2]

The French Data Protection Authority (the "**CNIL**") has recently issued a regulation on Biometrics processed in the work place for the purpose of access control[3] (the "**Regulation**"). Though PoPIA is not fully in force yet, but it will be soon. Employers using their employees' biometric data for clocking systems or other access control processes will have one year from that effective date to ensure thay they are fully compliant with PoPIA.

Here are a few interesting points in this Regulation, which give practical guidance on how any employer can design and use its biometrics access control systems to be compliant with the most stringent privacy regulations:

1- Justification of the biometrics processing for access control: principle of proportionality

The need to control access to business premises is legitimate for an employer. However, the means used to ensure such control have to be proportionate to the objective.

The employer has to justify, in a very concrete way, its need to implement a biometric system as opposed to other less intrusive access control solutions.

Both the specific status of the biometric data and the particular risks inherent in its processing limit the assumptions in which a controller can actually use biometric access control devices in the workplace.

It is up to the employer to:

– justify a specific context requiring a high level of protection, for example the handling of particularly dangerous machinery or products, access to funds or valuables, equipment or products subject to regulation specific (psychotropic substances and their precursors, chemicals that can be used for weapons, etc.);

– demonstrate the inadequacy of less intrusive means such as a badge or access code (for example, an environment in which strong identification is necessary to prevent identity theft in the event of theft of a badge or interception of access codes).

2- Which biometrics data can be used for access control

The Regulation provides that the individual’s morphological characteristics is authorized. However, biometric authentication requiring biological sampling (saliva, blood, etc.) is prohibited by the Regulation.

The choice of the types of biometry (iris, fingerprint, etc.) must be justified and documented by the employer, including the reason for using one biometric characteristic over another.

3- Conservation of biometrics data

The recordings (photo, audio recording, etc.) of a particular biometric can only be processed for the time required to calculate the sample and can not be stored.

The derived biometric data can only be stored as encrypted samples that do not allow the original biometric characteristic to be recalculated. They may only be kept for the duration of the data subject’s access authorization and must be deleted if the access authorization is withdrawn or if the person concerned ceases to work in the organization.

This is in line with the principle of minimization.

4- Is consent of the employee required?

The employee's consent should not be necessary.

Indeed, for a consent to be valid, the GDPR requires that it is given freely, in addition to being specific, informed and materialized by a positive action of the person[4]. However, in the workplace, the existence of the hierarchical link between the employer and the employee may affect the free nature of consent: This is why consent should very rarely be retained as the legal basis for data processing in the workplace (should this data be of biometric nature or not).

It is advisable to choose another legal basis, such as compliance with a legal obligation or, more frequently, the legitimate interest of the data controller/responsible party.

However, an employer deciding to rely on the consent of employees will have to make sure that there is a real freedom of choice for them: an equivalent alternative solution (badge, password, etc.) should be offered to employees so that they can choose the option that suits them best, without any consequences (negative or positive) influencing this choice.

This reduces substantially the practical advantages of implementing a biometrics access control system.

5- Security safeguards

Security safeguards should be sufficiently robust given the sensitive nature of data processed.

The Regulation provides for a very detailed and comprehensive list of measures (technical and organisational). These are only a few of the measures that the data controller/responsible party should adopt as a minimum:

– Measures relating to the biometric data:

o partition the data during transmission and retention;

o encrypt biometric data, including templates, using an algorithm cryptographic and key management in accordance with the state of the art. An encryption and key management policy must be clearly defined;

o prohibit any external access to the biometric data (for example by implementing measurements of card comparison type ("match-on-card") or physical security module / logic type HSM (Hardware Security Module).

– Measures relating to the organisation:

o make available an alternative "emergency" device to be used in exceptional circumstances, without any constraint or extra cost for employees who do not use the biometric solution; in particular, for people who do not meet the constraints of the biometric device (impossible to enrol or read the biometric data, handicap situation making it difficult to use, etc.) and in anticipation of the unavailability of the biometric device (such as malfunction of the device), a "backup solution" must be implemented to ensure continuity of the proposed service, limited however to exceptional use;

o strictly manage physical and logical access to devices and databases given by the authorized persons; in particular, a management policy foresights and access must be clearly defined; this is about formalizing the different categories of authorized persons (users, administrators and database managers, people in charge of data management, technical maintenance persons, etc.), their access rights, and access rights management, etc.

6- Data Protection Impact Assessment

The Regulation provides that a data protection impact assessment must be carried out by the employer prior to implementation of the biometric system[5].

The employer should document the risks and estimates them in terms of severity and likelihood. In accordance with the Regulation, the employer must update this risk assessment and any additional security measures implemented at least once every three years.

For more good, clear and precise advice, please do not hesitate to contact us.

[1] Biometrics, Wikipedia

[2] Art. 9 GDPR – Processing of special categories of personal data, Ar. 26 PoPIA – Prohibition on processing of special personal information.

[3] https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf

[4] Art. 7 GDPR, Conditions for consent.

[5] Art. 35 GDPR – Data protection impact assessment.