The need to review the implementation of technologies for the use of biometric data for time and attendance or access control

On 27 November 2023, the AEPD published a guide on the processing of time and attendance control using biometric systems, which puts the use of these technological tools at risk

Article 4(14) of the GDPR defines biometric data as "personal data obtained from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that person, such as facial images or dactyloscopic data". According to this definition, biometric data are all data that allow the identification or authentication of a person.

Companies that use this type of technology to comply, for example, with the registration of the working day or for access control for both work and non-work purposes, should review their use, given that the AEPD has modified the interpretation on the typology of data that it gave to biometric data in which, in accordance with the guide published by the AEPD on the processing of personal data in labour relations, dated 18 May 2021, it considered that the processing of biometric data in cases of one-to-one identification are not special categories of data, in which case they may be used for compliance with a legal obligation or for the performance of a contract.

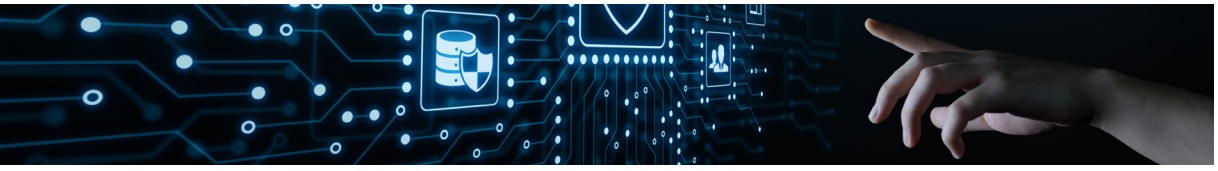
Based on the Guidelines published by the European Data Protection Board on 26 April 2023, the AEPD has revised its interpretation because, according to these Guidelines, both biometric identification and biometric authentication are processes that involve the processing of special categories of data.

This means that the established criteria are reinforced, and organisations will have to review the impact assessment, which was carried out at the time, in order to prove that the use of these tools passes the suitability, necessity and proportionality of the processing and the technical, organisational and legal measures implemented until now will have to be reviewed in order to be reinforced.

The AEPD classifies the use of biometric data as an independent "High Risk" data processing as it considers that these are special categories of data in accordance with article 9.1 of the GDPR, which as a general rule establishes the prohibition of the processing of special categories of data, unless we are dealing with one of the cases envisaged in number 2 of the aforementioned article 9.

In the case of time recording and access control for employment purposes, in order to overcome the lifting of the prohibition provided for in Article 9.1, we could consider the provisions of letter b) of number 2 of Article 9 to be applicable, which expressly states:

"(b) processing is necessary for the purposes of the performance of obligations and the exercise of specific rights of the controller or of the data subject in the field of employment law, social security and social protection, in so far as authorised by Union law of the Member States or by a collective agreement under the law of the Member States providing for appropriate safeguards for the respect of the fundamental rights and interests of the data subject".



The lifting of the prohibition could therefore be applied on the basis of the fulfilment of a legal obligation of the controller in the field of employment, safety and social protection, insofar as this is authorised by a rule having the force of law, whether laid down by the European Union or by the law of one of the Member States, or by a collective agreement, provided that measures are taken which respect the fundamental rights and interests of the data subject.

The applicable legislation would be RDL 8/2019, of 8 March, article 10 of which regulates the obligation to record the working day as a way of combating precarious employment and establishes the modification of article 34 of the Workers' Statute, adding a new section 9 which reads:

"...The company shall guarantee the daily record of the working day, which must include the specific start and end times of the working day of each worker, without prejudice to the flexible working hours established in this article. By means of collective bargaining or company agreement or, failing this, by decision of the employer after consultation with the legal representatives of the workers in the company, this attendance register shall be organised and documented. The company shall keep the records referred to in this provision for four years and they shall remain at the disposal of the workers, their legal representatives and the Labour and Social Security Inspectorate".

For the AEPD, this legal obligation to implement a working time register does not legitimise or protect the processing of biometric data, given that the regulation does not refer to the use of biometric data to keep the working time register and, since the data in question belong to special categories of data, it is necessary for it to be established in a legal regulation.

In relation to access control for work purposes it is article 20.3 of Royal Legislative Decree 2/2015, of 23 October, approving the Revised Text of the Workers' Statute Law, which states that:

"3. The employer may adopt the measures it deems most appropriate for monitoring and control to verify compliance by the worker with their work obligations and duties, keeping in their adoption and application the consideration due to their dignity and taking into account, where appropriate, the actual capacity of workers with disabilities".

However, as in the previous case, this article does not mention the use of biometric data to establish access control.

This interpretation is also included in Opinion 1/2023 issued by the Transparency and Data Protection Council regarding the processing of biometric data through the use of facial recognition and/or fingerprint devices for the time control of City Council staff, in which it states that Spanish legislation does not contain any specific authorisation to consider the processing of biometric data necessary for the purpose of time control or access control for employment purposes.

Based on this, we can conclude that organisations should review the criteria based on which they decided to implement this type of tool on the basis of the following points:

(i) Analyse the implementation criteria in order to ensure that they pass the adequacy, necessity and proportionality data protection test.

(ii) Identify that there is a circumstance for lifting the prohibition on processing special categories of data and a condition that legitimises the processing, which cannot be based on consent.

(iii) Any use of biometric data must have its own circumstance for lifting the prohibition on processing.

(iv) Once the Data Protection Judgment has been passed, organisational, technical and legal safeguards must be implemented, and a risk analysis carried out.

For further information, please contact:

María Suárez
Partner | Privacy & Intellectual Property
maria.suarez@es.Andersen.com