Alicia Maddio and Isabel Iglesias

Beyond fingerprints: Understanding the AEPD's Guide to Attendance Monitoring with Biometric Systems

About the Guide "Processing of attendance monitoring using biometric systems"

In the era of digitalisation and technological innovation, methods used to monitor attendance are evolving rapidly. In this regard, one of the most widely debated emerging technologies is the use of biometric systems. In this context, on 23 November, the Spanish Data Protection Agency ("**AEPD**") published the Guide "Processing of attendance monitoring using biometric systems", a document that addresses in detail the criteria for the processing of attendance monitoring -both inside and outside the workplace- using biometric systems, as well as their compliance with the General Data Protection Regulation ("**GDPR**").

In this legal briefing, we will break down the most important aspects of the Guide, providing a concise analysis of its contents, in order to make it easier for organisations and their managers to understand and apply these guidelines in their attendance monitoring systems.

What are biometric data and systems?

Biometric data processing systems are based on the collection and processing of personal data relating to the physical, physiological or behavioural characteristics of natural persons, enabling their identification, tracking or profiling ("**processing**"[1]).

Biometric data[2] is personal data obtained from a specific technical process, which relates to the physical, physiological or behavioural characteristics of a natural person and which **allows or confirms** his or her unique identification. This type of data is covered by Article 9.1 of the GDPR, which contains a general rule prohibiting the processing of personal data that reveals, *inter alia*, biometric data intended to uniquely identify a natural person.

How has the AEPD's position changed in this respect?

In 2021, the AEPD published the guide "Data Protection in Labour Relations[3]". In the section "Biometric data", this guide addressed the use of biometrics in the implementation of attendance register processing. **This guide noted that biometric authentication[4] was outside the special categories of data**.

However, this interpretation has been modified by the Guidelines 05/2022 of the European Data Protection Board ("**EDPB**"), on the use of facial recognition technology in the area of law enforcement[5], meaning that the interpretation offered by the AEPD in the Guide analysed here seeks to adapt to this context, and, therefore, considers biometric authentication to be a process involving the processing of special categories of personal data.

1. Art. 4.2 of the GDPR
2. Art. 4.14 of the GDPR
3. Available at: https://www.aepd.es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf
4. In particular, the AEPD established that biometric data is only considered a special category of data in cases where it is subject to technical processing aimed at biometric identification (one-to-many) and not in the case of biometric verification/authentication (one-to-one).
5. Available at: https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

What are the most relevant aspects of the published Guide?

- The Guide notes that **current Spanish legislation does not contain a sufficiently specific authorisation to justify the need to process biometric data for the purpose of monitoring the timetable of the working day (start/end of the working day and access monitoring for work purposes)**.
- **The consent of the data subject**, in the case of the processing of working time registration with biometric techniques, **does not generally remove the prohibition on processing**, due to an unbalanced relationship with the data controller - which occurs in the context of an employment or administrative/public service relationship - and, therefore, would not pass the test of necessity required for high-risk processing. However, **where there are truly equivalent options available** to all employees, **consideration could be given** to whether consent would be valid.
- Regarding access monitoring for non-work purposes, it will be necessary to **demonstrate the objective necessity of the processing, as well as possible alternatives**, i.e., in order to process biometric data, there must be no other alternative that meets the identified need.
- It will not be possible to use the biometric identification or authentication process in those cases of attendance monitoring with **automated decisions**, which do not allow for human intervention with the power to reverse the decisions taken.
- Before any decision is taken to implement an attendance monitoring system using biometric systems, it is necessary to carry out risk management[6] by design and by default[7], applying appropriate technical and organisational measures to ensure and be able to demonstrate that the processing complies with the GDPR. In the case of high-risk processing, a Data Protection Impact Assessment ("**DPIA**[8]") must be successfully completed.
- For biometric systems that are implemented using artificial intelligence techniques, it is essential to consider their classification "high risk "[9].

What *minimum* measures should be applied to the processing of attendance monitoring?

The AEPD lists a series of **minimum measures by default**[10] that can be extended to the processing of attendance monitoring. These measures are as follows:

1. Inform data subjects about the biometric processing and its risks.
2. Implement an option in the biometric system to remove the identity link between the biometric template and the natural person.
3. Implement technical measures to ensure that it is impossible to use the templates for any other purpose.
4. Use encryption to protect the confidentiality, availability and integrity of the biometric template.
5. Use specific data formats or technologies that make the interconnection of biometric databases and the disclosure of unverified data impossible.

6. Art. 24.1 of the GDPR

7. Art. 25 of the GDPR

8. The DPIA must include and pass the triple test of suitability, necessity and proportionality of Art. 35.7.b of the GDPR, also provided for by the doctrine of the Constitutional Court.

9. As stated in Annex III to the Proposal for a Regulation laying down harmonised rules on artificial intelligence. The Proposal for a Regulation is currently being discussed by the Parliament and the Council in the presence of the European Commission, in so-called tripartite dialogues ("*trilogues*"), thus following the ordinary legislative procedure of the European Union.

10. Already established by the AEPD, in the section "Biometric data" in the guide "Data Protection in Labour Relations", available at: https://www.aepd.es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf (date of last access: 24/11/2023).

6. Delete biometric data when it is not linked to the purpose for which it was processed.
7. Implement data protection by design.
8. Conduct a DPIA.

CONTACTS

Raúl Rubio
Partner, Intellectual Property and Technology
rrubio@perezllorca.com
T. +34 91 353 45 59

Andy Ramos
Partner, Intellectual Property and Technology
aramos@perezllorca.com
T. +34 91 423 20 72

Yolanda Valdeolivas
Of Counsel, Employment, Compensation and Benefits
yvaldeolivas@perezllorca.com
T. +34 91 389 01 80