AUGUSTA
ABOGADOS

January 2024

RESTRICTIVE INTERPRETATION OF THE SPANISH DATA PROTECTION AUTHORITY REGARDING THE USE OF BIOMETRIC SYSTEMS FOR TIME & ATTENDANCE CONTROL

In the framework of data protection in the European Union, the Spanish data protection authority, named Spanish Data Protection Agency (AEPD), has recently published a guide addressing the processing of biometric data in the context of time and attendance control. This guide seeks to provide clear guidelines in line with the European Union's General Data Protection Regulation (GDPR), specifically Regulation (EU) 2016/679 of the European Parliament and of the Council, which governs the processing of personal data.

Biometric data, obtained through systems such as fingerprints or facial recognition, are considered "special category" data according to Article 9 of the GDPR, and the AEPD identifies the processing of these data in time and attendance control as a high risk to fundamental rights and individual liberties.

The guidance sets out the essential requirements that must be met for the lawful processing of biometric data, including the need to lift the prohibition on processing of special data under the GDPR (Article 9.2) and obtaining the adequate legitimation (Article 6). In addition, it is emphasised the importance of the principles of minimisation and necessity, ensuring that the purpose of the processing cannot be reasonably achieved by other means.

Regarding consent, the guide highlights that, in general, consent is not considered free due to possible inequalities in employment relationships. It underlines that only in specific situations, such as time recording, such consent could be considered as free if there are alternatives without risks to the employees' rights. However, if such alternatives exist, the principle of necessity of biometric systems would not be fulfilled.

This document marks a departure from a previous guide issued by the AEPD in May 2021, by highlighting the importance of explicit employee consent and the necessity for the processing, even in the context of employment obligations. In addition, it addresses biometric identification and authentication as processes that also involve the processing of special categories of personal data.

The current guide states that the exception to the prohibition of processing special data regarding Article 9 GDPR in the field of employment shall not apply. Moreover, it highlights the need for a prior analysis demonstrating that there are no equally effective and less intrusive means of recording presence, the principle of necessity and minimisation in the processing of personal data.

The contents of this publication are for information purposes only and should not be relied upon as a basis for making a decision, in which case specific legal advice should be sought

Given the risk associated with the processing of biometric data, the AEPD states the obligation to carry out a Data Protection Impact Assessment (EIPD), considering the criteria of appropriateness, necessity, and proportionality. Proactive accountability under the GDPR requires not only passing the EIPD, but also documenting and being able to prove the organisational, legal, and technical measures taken.

In addition, the guide prohibits the use of biometric time and attendance systems based on automated processes without human intervention, unless the processing is based on the essential public interest or compliance with a legal obligation. In the case of time recording by means of biometric systems, the inclusion of guarantees in collective bargaining agreements is suggested, although this does not exempt from compliance with other measures and from carrying out the triple test together with the EIPD.

The AEPD also proposes a set of additional measures to be implemented if all the necessary requirements are met to ensure compliance with the GDPR principles. These measures include informing data subjects about the biometric processing and the associated risks, allowing the revocation of the identity link between the biometric template and the individual, limiting the use of the templates to the informed purposes, encrypting the templates, and using specific technologies that prevent unauthorised interconnection of biometric databases.

In the event of non-compliance with these guidelines, the AEPD warns of possible sanctions that may range from warnings to temporary or definitive bans on processing, as well as fines of varying amounts, depending on the seriousness of the infringement. These fines, categorised as serious or very serious infringements, could reach up to 20 million €, or 4% of annual turnover, depending on the specific circumstances of each case.

It should be noted that the guidance also establishes a connection between the risk associated with the processing of biometric data and the development of these systems through Artificial Intelligence. This anticipates the possible regulation of biometric systems in the future Artificial Intelligence Act, projected to be approved in the coming years, and highlights the importance of aligning the processing of biometric data with the protection of personal data.

In summary, although the GDPR does not strictly prohibit the use of biometric systems for time recording, this guide issued by the Spanish AEPD introduces more detailed restrictions in its interpretation and in the exceptions that could allow such use, highlighting the importance of consent and the necessity for processing in these cases.

Corporate & Innovation Area | **Augusta Abogados**