GUIDELINES
CLOCKING AND ATTENDANCE CONTROL PROCESSING USING BIOMETRIC SYSTEMS

V. November 2023

INDEX

This document is a courtesy translation by the AEPD of the original legal report. In the event of any inconsistencies between the Spanish version and this English courtesy translation, please note that the Spanish version shall prevail.

I. INTRODUCTION

This document will determine the criteria for the processing of clocking and attendance control by means of biometric systems in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as "GDPR").

Biometric systems, and the processing of data obtained from them, are evolving very rapidly. The new systems increase the detail of the information collected, allowing the possibility of collecting information without cooperation from the person, sometimes without being aware of it. Through information available on the web and at greater distances, it is possible to process biometric information. The development of Artificial Intelligence makes it possible to infer additional information about the subject through even categories of sensitive data. Biometric data can be collected and used across multiple physical and internet services.

As a consequence, there have been changes in the regulatory, social and technological context, even in a short and recent period, which make it necessary to consider the limits to the processing of biometric data and the measures that must be established so that a processing of personal data that decides to use biometric systems ensures compliance with the GDPR or other regulations that affect these systems, such us the case of being based on artificial intelligence techniques, such as the future European Regulation on Artificial Intelligence.

A. BIOMETRIC SYSTEMS AND DATA

Biometric data processing systems are based on collecting and processing personal data relating to the physical, physiological or behavioural characteristics of natural persons, including, as has recently been shown, their neural characteristics, by devices or sensors, creating biometric templates (also known as signatures or patterns) that enable identification, tracking or profiling of such persons (i.e., "processing", Art. 4(2) GDPR).

The GDPR defines in Art. 4(14) 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 natural person, such as facial images or dactyloscopy data;"[1]. The definition establishes that biometric data is all data that allows the identification or authentication of a person.

B. THE BIOMETRIC TEMPLATE AS PERSONAL DATA

Art. 4(1) GDPR defines personal data as:

> *(1) 'personal data' means any information relating to an identified or identifiable natural person ('the data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

To identify a person, as follows from that provision, is to determine the identity, directly or indirectly, of the person. Assigning an identifier is, therefore, a process that makes it possible to single out an individual and, therefore, the actions aimed at him. In particular, among other

[1] The bold type is not in the original text.

possible means, through "*elements of physical, physiological, genetic, and psychic identity*." In this sense, a processing that makes possible to single out a person among several by using, for example, a process of biometric behavioural analysis that uniquely differentiates and points to a person, is an identification processing.

Recital 51, in relation to biometric data, explains:

> *The processing of photographs should not be systematically considered to be processing of special categories of personal data, as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.*

A photograph, when captured and stored in a digital system, is encoded in a standard format using zeros and ones. The type of encoding used is aimed to be able to reproduce the image so that it can once again be understood by a human. Thus, recital 51 of the GDPR, when it states that the processing of photographs *"(...) should not be **systematically** considered to be processing of special categories (...)*", what it is meaning is that the content of that photograph or a further processing ***may become*** a processing of special categories of data[2].

A biometric data contained in a system is stored in a biometric template or pattern format. A biometric template is a way of writing a human biometric feature, such as a face or a fingerprint, in a way that is efficiently and effectively interpretable by a machine for a given purpose or purposes. The biometric template is not intended to be interpreted by a person, like a photograph, but is oriented to be processed in an automated process, i.e., to be efficiently and effectively interpretable by a machine. This type of storage would make it possible to single out an individual and perform actions automatically, profile or infer information about a subject such as attitudes or patterns of behaviour, etc.

In the case of identification or authentication operations, for a biometric template to be effective, it is necessary that the templates generated from two different individuals are clearly distinguishable. In that case, the template acts as a unique identifier for the person. The fact that, based on a biometric template (e.g.) for facial recognition, the original face cannot be reconstructed is irrelevant, since it is a unique identifier that uniquely singles it out, at least in the context of automated processing. In the same way, it is not possible to reconstruct a name or a face from the national ID or passport number alone. Both unique identifiers, biometric template or ID number, can be associated with additional personal data and attributes in a file. Unlike an ID number, the biometric template is not assigned to a person by a third party but is generated directly from the observation of unique and unalterable physical characteristics of the individual himself, without the need to resort to documents, other devices or databases of third parties.

Therefore, a biometric template for identification or authentication purposes is personal data per se and a unique identifier[3].

---

[2] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) Explanatory Report, paragraph 60 "Processing images of persons with thick glasses, a broken leg, burnt skin or any other visible characteristics related to a person's health can only be considered as processing sensitive data when the processing is based on the health information that can be extracted from the pictures."

[3] Article 29 Data Protection Working Party. WP80 Working document on biometrics, adopted on 1 August 2003. Paragraph 3.8 Unique identifier

C. CLOCKING AND ATTENDANCE CONTROL PROCESSING

Clocking and attendance control is a processing that can be used to achieve different purposes and is subject to be compliance with data protection regulation, and without prejudice to the specificities of the regulations to be applied in each case.

On the one hand, the registration of working hours, or clocking, is a processing that would be legally framed within an employment relationship, with the purpose of monitoring its performance. On the other hand, attendance control would be linked to the purpose of supervising the entry and/or exit to certain premises. The latter may or may not be carried out within the scope of work and for work purposes. Both, in terms of processing personal data, must comply in any case with the principles, rights and obligations established in the GDPR. Implementing them using a biometric system also entails additional considerations for GDPR compliance.

Registration of working hours

In relation to the registration of working hours or clocking, Royal Decree-Law 8/2019, of March 8, 2019, on urgent measures for social protection and the fight against job insecurity during working hours, establishes in Chapter III "*Measures to combat job insecurity during working hours*", and in its article 10 regulates the registration of working hours as a way of combating job insecurity, by amending article 34 of the revised text of the Workers' Statute Law (hereinafter referred to as ET), approved by Royal Legislative Decree 2/2015, of 23 October, adding a new section 9, with the following wording:

> *'9. The undertaking shall ensure that the daily working day is recorded, which must include the specific start and end times of each worker's working day, without prejudice to the flexible working hours provided for in this Article.*
>
> *By means of collective bargaining or company agreement or, failing that, a decision of the employer after consultation with the workers' legal representatives in the company, this attendance record will be organized and documented.*
>
> *The company shall keep the records referred to in this provision for four years and they shall remain available to the workers, their legal representatives and the Labour and Social Security Inspectorate.'*

As specified in section V of the Explanatory Memorandum of the aforementioned Royal Decree Law 8/2019, the purpose of the established obligation is to guarantee compliance with the limits on working hours, to create a framework of legal certainty for both workers and companies and to enable control by the Labour and Social Security Inspectorate, as a means of correcting the situation of precariousness, low wages and poverty that affects many of the workers who suffer abuses in their working hours.

Attendance control for working purposes

In relation to access control for working purposes, this is usually based on the provision contained in article 20(3) of ET, which establishes that:

> *"3. The employer may adopt the measures it deems most appropriate for monitoring and control to verify the worker's compliance with his or her labour obligations and duties, taking into account the dignity of the worker in their adoption and application and taking into account, where appropriate, the real capacity of workers with disabilities."*

Attendance control for other purposes

Regardless of the mandatory nature of the registration of working hours or clocking for work purposes, there are cases in which it is also necessary to carry out a presence control that does not necessarily have to do with an employment relationship. In this situation, the aim is to achieve a different purpose, which consists of supervising the access of users or customers to certain premises or spaces, or that is necessary for the performance of a contract for, for example, the enjoyment of certain services.

II. PRINCIPLE OF DATA MINIMIZATION AND DATA PROTECTION BY DESIGN

One of the principles of the GDPR is the principle of minimisation, which states in Art. 5(1)(c) that the data shall be:

> *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'('data minimisation');"*

Recital 39 explains very clearly that data that is not necessary for the purpose of the processing should not be processed:

> *"(...) Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means (...)"*

The data processed must be limited to what is necessary to achieve the purposes of the processing. In the present case, the purpose of a time and attendance control processing is not to process biometric data[4].

The application of this principle extends both to the obligation to consider the condition of necessity and also to take into account (Art. 24(1) GDPR) the risks to the rights and freedoms of natural persons, as set out in Art. 25(1) of the GDPR:

> *1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

A. MINIMIZATION IN THE PROCESSING OF CLOCKING AND ATTENDANCE CONTROL

In accordance with the provisions of articles 5(1)(c) and 25(1), in a clocking and attendance control processing, only the data necessary for the achievement of these purposes must be processed and not more than necessary. Likewise, this minimization must be applied when the processing, among others and as happens when biometric systems are involved, implies a risk to the rights and freedoms of natural persons.

Therefore, the need for additional data processing (in this case biometric data) must be justified when the same purposes have been achieved, and can be achieved, with another type of implementation that means equivalent and less intrusive data processing.

[4] There are processing in which the use of biometric data is part of their purpose, such as processing related to the investigation of biometric techniques, where the condition of necessity would be met.

It is not obligatory, nor advisable, that the implementation of a processing be limited exclusively to the selection of technological resources. In the options for implementing a processing, it is necessary to consider, among others, the use of human resources, legal guarantees, and organizational procedures. Therefore, in the evaluation of the equivalence and less intrusive alternatives, options that are not only technical should be assessed.

B. MINIMIZATION OF BIOMETRIC INFORMATION COLLECTION TECHNIQUES

The various products available on the market for the collection of biometric data that record such data with a precision, detail or frequency that is far above the needs of a given specific processing, violate the principle of minimization.

In many cases, simply because technology allows it and it is affordable, these products collect much more information than is actually necessary for the purpose of the processing, or in much more detail. The fact that a technology makes it possible to extract more information than the data necessary for the purpose of the processing does not justify its use. In the selection of technologies for the implementation of processing operations, the principle of data minimisation (Art. 5(1)(c) GDPR) must be followed, which determines that personal data must be only adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, so that personal data should only be processed if the purpose of the processing could not reasonably be achieved by other means (Recital 39). Even if the use of biometric operations and the lifting of the prohibition on processing special categories of data (Art. 9(1) GDPR) are fully justified and legitimized, when the controller chooses a certain biometric technology to implement the clocking and attendance control processing, it has to apply the principle of data minimization by design (Art. 25(1) GDPR), to this end, select and/or configure the system to suit the specific needs of the processing, and evaluate or obtain an objective evaluation resulting that there is no collection of data that is unnecessary for the purpose of the processing, in particular special categories of data (Art. 35 GDPR).

Therefore, in biometric systems for clocking and attendance control, an objective assessment on whether excessive data is being collected for the purpose of the processing must be carried out (see section IV.B of this document).

III. BIOMETRICS IN A CLOCKING AND ATTENDANCE PROCESSING

Art. 4(2) GDPR defines "processing" as:

> *" any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"*

The purpose of the GDPR (Art. 1) is to lay down the rules on the protection of natural persons with regard to the processing of personal data and the rules on the free movement of such data.

The Court of Justice of the European Union (hereinafter CJEU) has established a broad interpretation of both the concept of "personal data" and the concept of "data processing", in pursuit of the stated objective of the GDPR to ensure a uniform and high level of protection of natural persons within the Union and to strengthen and specify the rights of data subjects (recitals 10 and 11 GDPR, and paragraph 55 of the CJEU judgment of 22 June 2023, C-579/21, Pankki S).

Thus, in paragraphs 42 to 46 of the judgment in Case C-579/21, Pankki S, cited above, the CJEU states:

> *42 The use of the expression 'any information' in the definition of the concept of 'personal data' in that provision (Article 4(1) GDPR)) is evidence of the EU legislature's objective of attributing to that concept a very **broad** meaning, which may cover all types of information, both objective and subjective, in the form of opinions or assessments, provided that they are 'about' the person concerned (judgment of 4 May 2023, Österreichische Datenschutzbehörde and CRIF, C487/21, EU:C:2023:369, paragraph 23).*
>
> *43 In that regard, it has been held that information relates to an identified or identifiable natural person where, by reason of its content, purpose or effects, the information relates to an identifiable person (judgment of 4 May 2023, Österreichische Datenschutzbehörde and CRIF, C487/21, EU:C:2023:369, paragraph 24).*
>
> *44 As regards the 'identifiable' nature of a person, recital 26 of the GDPR states that 'account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly'.*
>
> *45 It follows that the broad definition of the concept of 'personal data' covers not only data collected and retained by the controller, but **also includes all information resulting from the processing of personal data** relating to an identified or identifiable person (see, to that effect, judgment of 4 May 2023, Österreichische Datenschutzbehörde and CRIF, C487/21, EU:C:2023:369, paragraph 26).*
>
> *46 In the second place, as regards the concept of '**processing',** as defined in Article 4(2) of the GDPR, it should be noted that, by using the expression 'any operation', the EU legislature intended to give that concept a broad scope, by using a **non-exhaustive list of operations applied to personal data** or sets of personal data, comprising, inter alia, collection, recording, storage or even consultation (see, to that effect, judgment of 4 May 2023, Österreichische Datenschutzbehörde and CRIF, C487/21, EU:C:2023:369, paragraph 27).*

A. BIOMETRICS AS ONE OF THE POSSIBLE MEANS TO IMPLEMENT THE PROCESSING

The techniques and technologies used in the implementation of a processing are part of the nature of the processing. The operations of a processing can be implemented in various ways: either manual or automated processing, and the latter in turn can be materialized with different technologies. Due to the complexity of the technologies available, these may imply that the scope of the processing is extended in terms of the categories of data processed, such as, for example, in the case of processing implemented on a web portal, which involves the collection of identifiers such as IP addresses, cookies, device signature, etc.

If the processing of personal data consists of the daily recording of the working day, clocking, a varied set of operations is required, including the identification of the employee, the collection of his/her personal data, its storage, the identification and authentication of the employee in the clocking process, the recording of time and other possible data (such as locations), its processing to determine overtime or shortages, its conservation, its making available to the Labour Inspectorate, etc.

Something similar occurs when what is intended is the control of attendance to certain places for purposes different than the work itself, since it is necessary to carry out a set of operations, although in this case it is not a question of identifying an employee for the purpose

of accounting his/her working hours, but simply to identify the entrance of a person and sometimes also his departure.

All these operations could be carried out using different human, technical and organisational means, either through the presentation of documents, the verification of their integrity, the comparison of shared information, the use of keys or certificates, the use of physical tokens, the behavioural analysis of the veracity of their statements, processing by means of automatic analysis of the movement of a mouse or other input/output device, etc. Biometric analysis of handwritten signature, fingerprint, hand, voice, facial recognition, iris, etc. Even with a combination of several of them, such as, for example, using different biometric systems (multibiometrics) with a greater or lesser degree of human intervention.

A controller for a time and attendance processing could decide, initially and to the detriment of other solutions, to use biometric systems to implement the time and attendance processing. In that case, biometric processing will not be final purpose by itself but a means to carry out operations within the processing. This choice made by the controller entails additional processing of data, in this case biometrics, for which it will be necessary to assess their compliance with the GDPR.

B. BIOMETRIC IDENTIFICATION AND AUTHENTICATION

Identification and authentication are operations that are not defined in the GDPR. However, they are defined in other European regulations such as Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation). Article 3 of eIDAS Regulation defines these terms as follows:

> *1 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;*
>
> *5 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;*[5]

In other words, this regulation considers authentication as an electronic process that makes identification possible.

In an informal or intuitive way, the concept of identification can be explained as the process by which a particular individual is recognized within a group, comparing the data of the individual to be identified with the data of each individual in the group (one-to-many). Verification or authentication would be the process of proving that an individual's claimed identity is true, comparing the individual's data only with the data associated with the claimed identity (one-to-one).

The first biometric identification or authentication operations in the biometrically implemented clocking and attendance control processing are carried out during the registration of the employee or during the registration of a person to be able to access a space or activity. In this process, it is necessary to identify the person correctly, otherwise the entire time and attendance control processing could be flawed. To this purpose, a series of creditable attributes of their identity are collected. Thus, the individual could be identified with the ID card and then additional data could be collected in the registration process, in

[5] The latest wording of the proposed amendment to the eIDAS Regulation provides for "authentication", an electronic process that makes it possible to confirm the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form;'

particular, their biometric data. But it could also be the case that the documents presented, for example, the ID card, are authenticated by biometric analysis of the correspondence of the photo of the ID card with the live image of the person, so that there would be an authentication operation (one-to-one). Or you could collect the biometric data first to identify it against a database storing attributes (such as name or ID number) in a one-to-many search, so you would have an identification operation.

A process of control of the person is then carried out on a regular basis with the aim of collecting their data on the start/end of the working day or entry and, where appropriate, exit from a certain place or space. In the case of using biometric systems, this can be done through an identification process, when biometric data is collected to compare it with a database in which the attributes of, for example, name or employee number (one-to-many) are stored. The process, in order to be an authenticated one, would have to be implemented in reverse, first the identification would be carried out through, for example, an ID card, and then the individual would be authenticated biometrically against the data stored in the system associated with the identity attributes.

Therefore, in a time and attendance control processing, whether for the registration of working hours or for attendance control (for work purposes or for other purposes), which uses biometric systems, there could be different implementation alternatives: either (i) based on two identification operations, (ii) based on one authentication and the other on identification, or (iii) based on a single authentication operation.

However, the casuistry could be even more complex for specific processing and the controller must describe in detail the biometric operations that are carried out within the framework of a record of working hours in each case.

C. ADDITIONAL PURPOSES IN A TIME AND ATTENDANCE PROCESSING BASED ON BIOMETRIC DATA

The biometric data collected within the framework of the clocking and attendance control processing may be used ("processed") for purposes other than the initial ones, since they are processing that, in short, identify a person in one way or another; For example, a record of working hours could be used for other issues: physical security, control of access to certain spaces or resources of the entity itself, evaluation of work performance, etc.

All these purposes, which are often presented as additional advantages to the decision to implement the processing of the registration of working hours or access control by biometric operations, must be considered processing for additional purposes. Therefore, the possibility of carrying out such processing depends on compliance with all the principles, rights and obligations set out in the GDPR.

IV. BIOMETRIC DATA AND SPECIAL CATEGORIES OF DATA

Article 9(1) of the GDPR lays down a general rule that prohibits the processing of personal data that reveals what it calls "special categories of personal data".

A. IDENTIFICATION AND AUTHENTICATION AS SPECIAL CATEGORIES OF DATA

Article 9(1) includes *"biometric data for the purpose of uniquely identifying a natural person" among* the special categories of personal data.

Recital 51, when referring to biometric data, interprets that concept as including data of such a nature where their processing by specific technical means allows the unequivocal identification or authentication of a natural person.

*The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of **biometric data** only when processed through a specific technical means **allowing the unique identification or authentication of a natural person**. Such personal data **should not be processed**, unless processing is allowed in specific cases set out in this Regulation, (...)"*[6]

Guidelines 05/2022 of the European Data Protection Board (EDPB) on the use of facial recognition in law enforcement (see Version 2.0 of 26 April 2023) determine, in paragraph 12, that the concept of biometric data encompasses both "authentication" and "identification", and although they are distinct concepts, in both procedures, data intended to identify a natural person is processed, so both are included in the concept of "data processing", and more specifically, they are processing of personal data of special categories. Consequently, the general prohibition established in Article 9(1) of the GDPR extends to both, so that this prohibition must apply not only to processing aimed at identification but also to cases of processing of biometric data aimed at authenticating or verifying the person with respect to the pattern previously established for the same.

In May 2021, the Spanish Data Protection Agency published the guide "Data Protection in Labour Relations", which addressed the use of biometrics in the implementation of attendance registration processing in the section "Biometric data" in chapter 4.6. The text interpreted biometric authentication outside of special categories of data. However, this interpretation has been superseded by the aforementioned Guidelines, so the interpretation of this AEPD must be adapted to the aforementioned EDPB Guidelines of 26 April 2023.

Similarly, the interpretation of these types of processing made by the AEPD in its Legal Report 036/2020, based, among other documents, on Opinion 3/2012 of the Article 29 Working Party (WP29), on the evolution of biometric technologies, - published at a time, 2012, when neither biometric data was considered a special category (only since the entry into force of the GDPR in 2016)-, it must also be considered to have been superseded by the EDPB's new position, as set out in those Guidelines 05/2022.

In short, it must be considered that, as in the case of identification, biometric authentication is a process that involves the processing of special categories of personal data.

B. BIOMETRICS AND THEIR LINKAGE WITH OTHER SPECIAL CATEGORIES OF DATA

The consideration of a special category of data should be interpreted broadly. Art. 9 (1) GDPR states that special categories of data are those that "***reveal***" certain types of information. The term "revealing" should be understood to mean that, in addition to data which by its nature contains sensitive information, data from which sensitive information relating to a person can be inferred are also special categories[7]. In the same way, the CJEU*'s conclusions "in relation to the purpose of the Directive, the expression "health-related data" used in Article 8(1) is also interpreted broadly to include information concerning all aspects, physical and mental, of an individual's health*".[8]

In this regard, the interpretation of biometric data as special categories of data should take into account the possibility that, through biometric analysis, other special categories of data can be inferred and collected, including health-related data or data revealing racial or ethnic origin.

---

[6] The bold type is not in the original

[7] Page 6 of the Article 29 Working Party Advice paper on special categories of data ("sensitive data").

[8] CJEU, 6 November 2003, Bodil Lindqvist, C-101/01, para. 50

Technological development is making it possible to extract more and more details from a person's biometric traits. For example, a biometric analysis of the human voice can collect more than a hundred different parameters that allow information to be extracted about health, physical or psychological problems, among others. In biometric systems based on facial recognition, data that reveals racial or ethnic origin can be processed[9], and health information, physical or psychological problems can also be extracted, as in the case of voice, even some fingerprint identification systems allow the recording of parameters such as temperature or blood pressure.

V. LIFTING OF THE PROHIBITION ON PROCESSING SPECIAL CATEGORIES OF DATA

The special protection established by the GDPR in its Art. 9 to certain categories of data derives from the impact that the processing of this data may have on the fundamental rights and freedoms of individuals.

Exceptions to the prohibition on the processing of special category data may only be made in the circumstances specified in Art. 9(2) of the GDPR. The controller is obliged to assess very seriously and diligently whether it has a solid reason for processing special categories listed in Art. 9(2) GDPR. The circumstances listed do not include legitimate interest, performance of a contract or pre-contractual measures.

A. EXCEPTION TO ART. 9(2)(B) GDPR: TIME AND ATTENDANCE CONTROL FOR THE REGISTRATION OF WORKING HOURS AND ACCESS CONTROL FOR WORK PURPOSES

Art. 9(2)(b) GDPR: Existence of a legal norm

Article 9 (2)(b) of the GDPR lifts the prohibition on the processing of special categories of data where:

> *"processing is **necessary** for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as **it is authorised** by Union or Member State law or a collective agreement pursuant to Member State law providing for **appropriate safeguards** for the fundamental rights and the interests of the data subject"*[10]

At the same time, it should be noted that the reference to authorisation by the law of the EU Member States must be understood as referring, in the case of the Spanish State, to the existence of a provision of legal status in accordance with the provisions of article 53.1 of the Spanish Constitution, as it deals with the development of a right, that of the protection of personal data, recognized as fundamental. In this regard, the judgment of the **Spanish Constitutional Court 76/2019**, of May 22, 2019, specifies that the legal norm must meet all the essential characteristics as a guarantee of legal certainty, **expressing each and every one of the presuppositions and conditions of the intervention**, so that the limitations of the fundamental right established by a law may violate the Spanish Constitution if they suffer from a lack of certainty and predictability.

Specifically, the Spanish Constitutional Court, in the aforementioned STC 76/2019, of 22 May, after citing, among others, its previous STC 292/2000, of 30 November, states:

---

[9] Article 29 Working Paper on Biometrics WP80 of 1 August 2003 paragraph 3.7 Sensitive data

[10] The bold type is not in the original.

- Secondly, by express mandate of the Constitution, any State interference in the field of fundamental rights and public freedoms, either directly affecting their development (art. 81.1 CE), or limiting or conditioning their exercise (art. 53.1 CE), requires a legal authorization (for all, STC 49/1999, of 5 April, FJ 4). In STC 49/1999, FJ 4, we defined the constitutional function of this reservation of law in the following terms:

This reservation of law to which, in general, the Spanish Constitution subjects the regulation of the fundamental rights and public freedoms recognized in Title I, has a twofold function, namely: on the one hand, it ensures that the rights that the Constitution attributes to citizens are not affected by any State interference not authorized by their representatives; and, on the other hand, in a legal system such as ours in which judges and magistrates are subject "solely to the rule of law" and there is, strictly speaking, no link to precedent (SSTC 8/1981, 34/1995, 47/1995 and 96/1996), it is, in short, the only effective way of guaranteeing the requirements of legal certainty in the field of fundamental rights and public freedoms. That is why, as far as our legal system is concerned, we have characterized legal certainty as a sum of legality and certainty of law (STC 27/1981, legal basis 10)."

This dual function of the reservation of law translates into a twofold requirement: on the one hand, the necessary intervention of the law to enable interference; and, on the other hand, this legal norm "must meet all those indispensable characteristics as a guarantee of legal certainty", that is, "it must express each and every one of the presuppositions and conditions of the intervention" (STC 49/1999, FJ 4). In other words, "not only does it exclude powers of attorney in favour of regulatory norms [...], but it also implies other requirements with respect to the content of the law that establishes such limits" (STC 292/2000, FJ 15).

The second requirement referred to above constitutes the qualitative dimension of the reservation of law and is embodied in the ***requirements of foreseeability and certainty of restrictive measures in the field of fundamental rights****. In STC 292/2000, FJ 15, we pointed out that, even if they have a constitutional basis, the limitations of the fundamental right established by a law "may violate the Constitution if they suffer from a lack of certainty and predictability in the limits they impose and their mode of application", since "****the lack of precision of the law in the material presuppositions of the limitation of a fundamental right is likely to generate an indeterminacy as to the cases to which a restriction applies****"; 'When this result occurs, beyond all reasonable interpretation, the law no longer fulfils its function of guaranteeing the very fundamental right which it restricts, since it leaves the will of the person who has to apply it to operate instead'. In the same judgment and legal basis, we also specified the type of infringement entailed by the lack of certainty and predictability in the limits themselves: "not only would it infringe the principle of legal certainty (Article 9.3 EC), conceived as certainty about the applicable legal system and a reasonable expectation of the person as to what the action of the power should be in applying the law (STC 104/2000, FJ 7, for all), but at the same time that such a law would be infringing the essential content of the fundamental right thus restricted, since the way in which its limits have been set makes it unrecognizable and makes it impossible, in practice, to exercise it (SSTC 11/1981, FJ 15; 142/1993, of 22 April, FJ 4, and 341/1993, of 18 November, FJ 7)"*[11].

[11] The bold type is not in the original

And in paragraph 16 of STC 292/2000, cited again by STC 76/2019, it is specified:

> *(...) It is the legislature that must determine when that good or right justifies the restriction of the right to the protection of personal data exists and in what circumstances it may be limited and, moreover, it is the legislator who must do so by means* ***of precise rules that make the imposition of such a limitation and its consequences foreseeable to the data subject****. Otherwise, the legislature would have transferred to the administration the performance of a function that is incumbent on it alone in matters of fundamental rights by virtue of the reservation of law in Article 53.1 EC, that is, to clearly establish the limit and its regulation.*

This means, as Opinion 2/2022 of the Catalan Data Protection Authority points out, that "*the impact on the right to data protection that derives from the regulation must be foreseeable*" and that "*the regulation cannot be considered foreseeable if it does not specify the possibility of using biometric data for the purpose of carrying out attendance control*".

This makes it necessary to reconsider the interpretation made by this AEPD in the section "Biometric data" of chapter 4.6 of the Guide "Data Protection in Labour Relations" of May 2021; and, as the Andalusian Transparency and Data Protection Council also concludes, in its Opinion 1/2023, "Regarding the processing of special categories of biometric data through the use of facial recognition and/or fingerprint devices for the time control of the staff of a City Council", the current Spanish legal regulations do not contain any sufficiently specific authorisation to consider the processing of biometric data necessary for the purpose of a time and attendance control of the working day. The sufficiently specific authorisation is not found for labour personnel, since articles 20.3 and 34.9 of the ET, do not contain such authorisation. Nor for personnel subject to an administrative legal relationship, as the provision related to the fulfilment of working hours referred to in article 54.2 of the revised text of the Law on the Basic Statute of Public Employees (hereinafter EBEP), approved by Royal Legislative Decree 5/2015, of 30 October, does not constitute a necessary authorisation.

Art 9(2)(b) GDPR: Necessity

Article 9(2)(b) of the GDPR, in relation to processing in the field of labour law and social security and protection, not only requires the existence of a legal authorisation – or collective agreement – but also imposes the requirement that the processing be "necessary".

Automatic time control systems have been around since 1890[12], and attendance registration has been done for several centuries through non-biometric means. To give an example, in the 80s of the twentieth century there were more than twelve million workers in Spain[13] subject to control of working hours. The largest vehicle factory in Spain had more than 30,000 workers at the time,[14] a figure that is now less than half[15]. In short, in the context of large volumes of workers, the employer had the power and capacity to establish a control of working hours.

The data controller, when proposing biometric operations, must justify the circumstances in which it *is no longer possible* to use the attendance registration systems that were being used in the same centre until that time, or that are being used in equivalent entities. In addition, you must justify that the use of other existing systems such as cards, certificates,

---

[12] https://en.wikipedia.org/wiki/Time_clock

[13] https://elpais.com/diario/1981/03/12/economia/353199602_850215.html

[14] https://infogram.com/evolucion-empleados-seat-1g4qpz7vxgd8m1y

[15] https://www.seat-mediacenter.es/smc/seat-sa/facilitiespage/martorell-production-facility#:~:text=En%20sus%2015%20edificios%20trabajan,por%20carretera%2C%20mar%20y%20tren.

passwords, *contact-less* systems, etc. that avoid the processing of special categories of data are not appropriate. Also, it must be taken into account that the processing of personal data may also rely on human intervention in its operations, i.e., there is no obligation for them to be implemented exclusively with technological means. Such human intervention may be the right complement to other options.

In the same way, the biometric information process must be *essential* to satisfy the fulfilment of the purpose of presence registration, as established in Opinion 3/2012 of the Article 29 Working Party, on the evolution of biometric technologies:

> *"(...) It is necessary to consider beforehand whether the system is necessary to respond to the identified need, i.e., whether it is essential to meet that need, and not just what is most appropriate or cost-effective. A second factor to be taken into account is the likelihood that the system will be effective in responding to the need in question in light of the specific characteristics of the biometric technology to be used."*

Therefore, the assessment of necessity must be overcome by means of objective evidence, with a broad vision of the context and avoiding being guided only by technological trends. Where the assessment involves elements other than the purpose of the processing or the protection of rights, such as economic constraints, employment, marketing techniques (such as impulse purchasing), or the possibility of obtaining consent for additional processing, a rigorous assessment of the proportionality of the processing must be carried out.

In conclusion, as indicated above, it is necessary to take into account Art. 5(1)(c) and recital 39 of the GDPR which states that personal data should only be processed if the purpose of the processing could not reasonably be achieved by other means. Again, it is pointed out that a prior analysis must be carried out on the necessity for such processing to achieve the intended purpose by the data controller, in the sense that there is no other equally effective and less intrusive means, before the implementation of any system; and all of this must be evaluated from the Principle of data protection by design, focusing the analysis on the rights and freedoms of the people whose data is going to be processed, within that first step. To this end, the corresponding risk analysis should be carried out and the impact assessment should be passed and the triple test of suitability, necessity and proportionality should be taken into account.

Art. 9(2)(b) GDPR: Suitability

In any case, the law that establishes the processing must respect the principle of proportionality, as recalled in the Spanish Constitutional Court Judgment 14/2003, of 28 January:

> *"In other words, in accordance with a reiterated doctrine of this Court, the constitutionality of any measure restricting fundamental rights is determined by strict observance of the principle of proportionality. For the purposes of the present case, it is sufficient to recall that, in order to determine whether a measure restricting a fundamental right satisfies the test of proportionality, it is necessary to ascertain whether it satisfies the following three conditions or conditions: whether the measure is capable of achieving the objective pursued (suitability test); whether, in addition, it is necessary, in the sense that there is no other more moderate measure for the attainment of that purpose with equal efficacy (judgment of necessity); and, finally, whether it is weighed or balanced, because it derives more benefits or advantages for the general interest than harm to other goods or values in conflict (proportionality judgment in the strict sense; STC 66/1995 of 8 May, F. 5; STC 55/1996, of 28*

March, FF. 7, 8 and 9; STC 270/1996 of 16 December, F. 4.e; STC 37/1998 of 17 February, F. 8; STC 186/2000 of 10 July, F. 6)."

As stated in Opinion 3/2012 of the Article 29 Working Party on the evolution of biometric technologies:

"(...) A second factor to take into consideration is whether the system is likely to be effective in meeting that need by having regard to the specific characteristics of the biometric technology planned to be used."

For a processing to be considered suitable, it must be able to fulfil the ultimate purpose of the processing with adequate levels of quality, taking into account that there is no processing that is free of errors or free from fraud.

To do this, it is necessary to define metrics, not only on the performance of the biometric systems, but also on the performance goals necessary in the processing for the recording of working hours. An objective analysis of the adequacy of the various technical options for attendance registration, including biometrics, is needed to meet these requirements.

In particular, it is necessary to determine whether there may be a lack of accuracy of the data obtained in relation to the biometric operation as it does not fit the average or standard human type according to the criteria of the controller. This can take the form of biases in profiling, incorrect identifications, identity theft, discrimination in population segments (the elderly, the disabled, racial types, the sick, etc.) or denial of access to services due to errors in data collection.

B. EXCEPTION TO ART. 9(2)(A) GDPR: TIME AND ATTENDANCE CONTROL FOR TIME REGISTRATION, ACCESS CONTROL (FOR WORK OR NON-WORK PURPOSES)

Consideration could be given to lifting the prohibition on the processing of biometric data due to the provision of *explicit* consent by the data subject for processing of such personal data for one or more of the specified purposes (unless expressly established otherwise by the law of the Union or its Member States), pursuant to Art. 9(2)(a) GDPR.

Article 4(11) of the GDPR refers to the consent of the data subject as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*". The information provided to the data subject is intended to, inter alia, make data subjects aware of the risks of such processing (recital 39 of the GDPR), especially when it affects people who are in a vulnerable situation[16].

There are processes that involve the use of biometric systems, other than clocking or attendance control, such as voluntarily participating in research on biometric identification techniques. In this case, the data subject could give consent to process their biometric data freely in order to participate as a test subject in said research. The purpose of such processing activity is to process biometric data. To be part of such project as a test subject must involve the processing of the biometric data.

[16] "They should also be informed on how the collection, use or sharing of facial recognition data is likely to affect them, especially when they concern persons in vulnerable situations. The information provided also has to state which rights and legal remedies the data subjects are entitled to." Guidelines on Facial Recognition. Consultative Committee of The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data - Convention 108

Registration of clocking and attendance control for work purposes.

In the processing of working time records, the employee has the obligation to participate in the processing whose purpose is the recording of the working hours. The purpose is not to processing biometric data. In this case, the consent does not apply to the processing of the working day registration itself, where it is not possible to object, but to the additional biometric data.

Thus, in the processing of the record of working hours and in relation to the freedom of consent for this additional processing of data, recital 43 of the GDPR establishes that:

> *"In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."*

The conditions for the consideration of consent are provided for in Art. 4(11) and 7 of the GDPR, and also Guidelines 5/2020 of the EDPB, on consent within the meaning of the GDPR, may also be used. In particular, they understand that in the context of employment relations, in general, there is an imbalance of power between employee and employer that means that this consent is not freely provided and should therefore not be the legal basis. For the sake of completeness, in that context, the consent of the data subject cannot, in any event, serve as a circumstance for the lifting of a prohibition on the processing of special categories of data. Thus, Guidelines 5/2020 states:

> *21. An imbalance of power also occurs in the employment context. Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, the EDPB deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee.*

A limitation on the use of consent is made explicit in the same Guidelines in relation to the use of consent in the framework of the Public Administrations:

> *16. Recital 43 clearly indicates that it is unlikely that public authorities can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities.*

However, the door is left open for the controller to demonstrate that there will be no adverse consequences for the data subject to withhold consent:

> *22. However, this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance*

of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent.

In the case of the recording of working hours, as the data subject has the obligation to record his/her working day, the existence of a free consent to additional processing of data, in this case biometrics, could only be considered if the data subject has an alternative to comply with that obligation. In this regard, the same Guidelines interpret:

37. The controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand. As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However, both services need to be genuinely equivalent.

Where there are truly equivalent options available to all employees, it could be analysed whether the consent is valid, complying with the requirements of Art. 4(11) of the GDPR and the rest of the conditions of Art. 7 of the GDPR.

However, with regard to this requirement of a possible "equivalent options ", it must be borne in mind that, if there are alternatives available to the processing of biometric data that involve less risk to the rights and freedoms of the persons, which allow all workers to opt for other alternatives at any given time, it means that the processing of biometric data is no longer *necessary* for the implementation of the processing.

As the processing of biometric data is not necessary, the provisions of art. 5(1)(c) of the GDPR would not be complied with, and as will be explained later in the chapter VIII of this document, being a high-risk processing, would therefore not meet the requirement of "*need*" imposed by Articles 5(1) and 35(7)(b). If the processing is high-risk, in addition to being necessary, the positive evaluation of *need* (Art. 35(7)(b) GDPR); which in this case would not be fulfilled, precisely because of that lack of necessity.

Therefore, in a processing of recording working hours implemented with biometric techniques, the consent of the interested party does not lift the prohibition of processing, in general, as there is a situation in which there is an imbalance with the data controller, as occurs in the context of an employment relationship (or administrative/civil servant). Additionally, it would not pass the assessment of necessity, a requirement for high-risk processing activities (see section VIII.A).

Access control for non-work purposes

A similar analysis could result for attendance control for purposes other than working. Consent must be free, specific, informed and unambiguous. Among other things, the controller must establish an alternative method to be able to carry out attendance control, without having any consequences for the person who does not want to use attendance control through biometric data processing.

As in the previous case, the objective necessity must be demonstrated (requirement for high-risk processing see section VIII.A) and possible alternatives, in such a way that in order to be able to process those biometric data there is no other alternative that serves to satisfy the identified need and that implies a lower risk to the rights and freedoms of natural persons.

VI. LAWFULNESS OF THE PROCESSING

If the prohibition on the processing of special categories of personal data, in this case biometrics, has not been lifted, it is irrelevant whether there is a legal basis provided for in Article 6(1) of the GDPR, since there is already a condition that invalidates the processing.

Once the prohibition has been lifted, it is necessary to analyse whether such processing is intended to be carried out within the framework of at least one of the conditions listed in Art. 6(1) of the GDPR. In other words, one should not propose a processing and then seek a condition of lawfulness. On the contrary, there should be a condition (the cause) defined in Art. 6(1) GDPR for a controller to decide to carry out processing (the effect).

A. PROCESSING THE TIME REGISTER

The recording of working hours is a legal obligation imposed on the employer and the employee (art. 34.9 ET), so the legal basis for the processing of the recording of working hours is in line with the provisions of art. 6(1)(c): *"the processing is **necessary** for compliance with a legal obligation applicable to the processing"* , in connection with the reiterated article 34.9 of the Spain's Workers' Statute Law (ET) which establishes the obligation for the company to guarantee a daily record of working hours that must include the specific start and end times of the working day for each worker.

In this case, if the lifting of the prohibition on further processing of biometric data has been carried out on the basis of the provisions of Article 9(2)(b) of the GDPR, there must be a rule with the force of law that protects this exception and, therefore, this rule will encompass the lawfulness of the processing in accordance with Article 6(1)(c).

It has already been indicated above that, for the purposes of lifting the prohibition of Article 9(2)(b) GDPR, the current regulations referred to above are not sufficient in the terms provided for in the GDPR.

On the other hand, instead of Article 9(2)(b) of the GDPR, it has been possible to consider lifting the prohibition of further processing of biometric data taking into account the provisions of Article 9(2)(a) GDPR. In this case, in order to be able to consider free consent, there must be, as has been explained, the possibility of implementing equivalent options. If these exist in the processing itself, or it is feasible to implement them, and are less intrusive in relation to the rights and freedoms of the data subjects, the requirement of "necessity" established in Article 6(1)(c) GDPR would not be met, as already developed in the previous section.

If the lifting of the prohibition on the processing of biometric data has been based on provisions other than Article 9(2)(a) and Article 9(2)(b), it is also necessary to ask whether there are other equivalent and less intrusive options for implementing the recording of working hours.

The reality is that, in the arguments of many decision-makers in basing the lifting of the prohibition on free consent when providing alternatives to the interested parties, they have made evident the possibility and viability of such alternatives. Therefore, even if the lifting of the prohibition was based on provisions other than those of Article 9(2)(a), this does not automatically imply that such alternatives do not exist. It may happen that the controller has decided not to implement the alternatives, in which case, the controller will have to objectively justify that in their specific case the biometric processing is necessary.

The same reasoning would apply to any of the legal bases provided for in Article 6(1) GDPR, from 6(1)(b) to 6(1)(f), as the requirement of necessity for the achievement of the purpose, which is set out in each of these legal bases, must always be met.

B. ACCESS CONTROL FOR WORK OR OTHER PURPOSES

In the event that the controller decides to base the lawfulness of processing biometric data on art. 6(1)(a) GDPR on attendance control processing for work purposes or for purposes other than work, then the conclusions reached in the section V.B of this text will apply.

In the case of substantiating the lawfulness of using biometric data in access control processing in other cases of Art. 6(1) of the GDPR other than consent, the requirements of necessity, present in all of them, will have to be met, in addition to those of reservation of law in letters (c) and (d) and also in the case of letter (f) the overcoming of the analysis of prevalence between the legitimate interests of the controller and the interests or fundamental rights and freedoms of the data subject that require the protection of personal data, in particular where the data subject is a child.

VII. AUTOMATED DECISIONS

Art. 22 GDPR provides for restrictions and safeguards when an automated process without human intervention produces legal effects on the data subject or similarly significantly affects him.

A clocking and attendance control processing could be implemented by the controller as an automated process based on a biometric system without human intervention that produces legal effects on the data subject or significantly affects him or her in a similar way. For example, when a system that controls attendance to the place denies such access for technical reasons and, by preventing access, and without the possibility of human intervention, automatically has an impact on the person, either on the worker's salary or employment, among others. Another example is that it prevents a data subject from accessing a certain activity or service previously contracted or that it limits their freedom of movement.

When the controller configures the attendance control processing in this way, it must be taken into account that, according to Art. 22 of the GDPR, cannot be based on special categories of data unless:

- The lifting of the prohibition is based on consent (Art. 9(2)(a) GDPR) or the essential public interest (Art. 9(2)(g) GDPR).
- And appropriate measures have been taken to safeguard the rights and freedoms and legitimate interests of the data subject. Such measures, at least (Art. 22(3) GDPR), must include:
    - The right to obtain human intervention from the controller,
    - To express their point of view and
    - To challenge the decision.

As Article 9(2)(a) of the GDPR does not apply, as explained above, nor Article 9(2)(g) of the GDPR, in the event that attendance control is considered as a processing in which there are automated decisions without human intervention with the competence to reverse the decision, a biometric identification or authentication process cannot be used.

VIII. RISK MANAGEMENT AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The lifting of the prohibition on processing special categories of data and the existence of a legitimacy for the processing does not conclude with the set of requirements that must be

met in order to determine that the processing is in compliance with the GDPR, and therefore that it can be carried out.

Among other requirements, it is essential that, prior to any decision to implement a time and attendance system through biometric systems, risk assessment is carried out (Art. 24(1) GDPR) and from the design and by default (Art. 25 GDPR) the appropriate technical and organisational measures are applied in order to guarantee and be able to demonstrate that the processing is in compliance with the GDPR. In particular, in the case of high risk, it must successfully pass a Data Protection Impact Assessment (DPIA) that must include to pass the triple judgment of suitability, necessity and strict proportionality established in Art. 35(7)(b) GDPR and also provided for by the doctrine of the Spanish Constitutional Court.

At the same time, it must be borne in mind that risk management for rights and freedoms does not exclude the prior obligation that there is a circumstance that allows the lifting of the prohibition on processing special categories, a condition that legitimises the processing, compliance with the conditions of Art. 22, with the principle of data minimisation and compliance with the principles, rights and other obligations set out in the GDPR.

A. HIGH RISK

High-risk processing is any processing that is likely, by its nature, scope, context or purposes, in particular if it uses new technologies, to pose a high risk to the rights and freedoms of natural persons.

One of the obligations of controllers is to assess the risk of their processing. The regulation already establishes the high risk of some processing, being a non-exhaustive list. Specifically, in development of the provision contemplated in the fourth section of article 35 GDPR, the obligation of the AEPD to publish the "Lists of types of data processing that require an impact assessment relating to data protection" is established, after their approval by the European Data Protection Board. They were included in these lists from a series of non-exhaustive criteria to determine the high risk of a processing.

A processing of attendance records that includes biometric data will be considered high risk because matches the criteria corresponding to numbers 4, 5 and 10 of the aforementioned lists. This list is not exhaustive for the evaluation of high-risk processing. Other characteristics related to the scope, context or specific nature of the implementation of the processing (e.g., use of multibiometrics, conditions of vulnerability of the data subjects, social situations, etc.), could restate the condition of high risk for the data subjects. For this reason, according to the criteria established in the guide "Data Protection in Labour Relations" of the AEPD, the processing of presence control using biometric techniques is also considered to be of high risk.

In Guidelines 3/2019 on the processing of personal data using video devices, Version 2.0 Adopted on 29 January 2020, by the European Data Protection Board, in section 5.1 "General considerations regarding the processing of biometric data" states the importance of risk assessment, of a necessity and proportionality assessment and the application of data minimization. These conditions, which are directly applicable to biometric operations using facial recognition in attendance control processing, can be extended to the use of other biometric systems to implement such processing:

> *73. The use of biometric data and in particular facial recognition entail heightened risks for data subjects' rights. It is crucial that recourse to such technologies takes place with due respect to the principles of lawfulness, necessity, proportionality and data minimisation as set forth in the GDPR. Whereas the use of these technologies can be perceived as particularly effective, controllers should first of all assess the*

impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing.

With regard to biometric systems that are implemented with artificial intelligence techniques, it will be necessary to take into account the classification of such systems as high risk according to Annex III of the proposal for the Regulation on Artificial Intelligence and compliance with the requirements that such systems will have to meet in order to be integrated into a presence registration process.

A high-risk processing will require the controller to pass, prior to the start of processing, the impact assessment relating to data protection established in Article 35 of the GDPR.

B. CARRYING OUT AND PASSING A DPIA

Passing a DPIA requires to demonstrate the suitability, necessity and proportionality of the processing and the proper management the specific risks of the processing by design, with the practical application of measures specifically aimed at minimising those risks, so as to ensure an acceptable risk threshold throughout the processing lifecycle, as established in Art. 35 GDPR. This would imply that, in accordance with the principle of proactive responsibility (Art. 5(2) GDPR), the controller must be able not only to demonstrate that the DPIA has been passed, but also to provide all the documentation prepared on the occasion of the implementation of the DPIA and justifying the results obtained in the DPIA and the organizational, legal and technical measures adopted in this regard. Documentation relating to the participation of the Data Protection Officer, if appointed, must also be included, among others. In addition, prior consultation with the supervisory authority will be mandatory in the event that the controller has not taken measures to mitigate the risk as required by Article 36 of the GDPR.

It should be borne in mind that risk assessment for rights and freedoms does not resolve the absence of a circumstance of lifting the prohibition on processing special categories, the non-existence of a condition of lawfulness, the non-compliance with the conditions of Article 22, the principle of data minimisation and the application of the principles, rights and other obligations set out in the GDPR.

The specification on how to comply with Articles 35 and 36 of GDPR has been developed by the AEPD in the following guidelines, which indicate how a DPIA must be executed and overcome, how it must be documented and how prior consultation must be carried out:

- Risk management and impact assessment in the processing of personal data
- Checklist for determining the formal adequacy of a DPIA and the submission of prior consultation
- Instruction 1/2021 of the AEPD of guidelines regarding the advisory function of the Agency. Chapter V: Prior Consultations [only available in Spanish]
- Template For Data Protection Impact Assessment Report (DPIA) For Public Administrations
- Template For Data Protection Impact Assessment Report (DPIA) For Private Sector
- Guidelines for Data Protection by Default
- A Guide to Privacy by Design
- GDPR compliance of processing that embed Artificial Intelligence
- GDPR compliance of processing that embed Artificial Intelligence. An introduction

In relation to biometric operations in clocking and attendance control process, these can use different systems, some simultaneously, and, in turn, the same biometric technique can

be implemented in different ways. Operations with biometric data in a specific processing will have a different degree of intrusion and impact on the privacy of individuals that will depend on the technique used, but also on the definition of the processing itself, its nature, the scope or scope in which it is to be carried out, its context, in particular, if the processing is configured as an automated decision.

The Spanish Data Protection Agency, in the guide "Data Protection in Labour Relations", in the section "Biometric data" in chapter 4.6, recommends some measures for general processing of clocking in/out using biometric systems to manage risk, which can be extended to attendance control in general:

- The use of biometric technologies should be based on the use of devices under the exclusive control of users.
- Preferably, centralized storage of biometric templates should not be used.
- Automated data suppression mechanisms should be implemented.
- In the case of attendance registration, the collective bargaining agreements must include the set of guarantees in relation to this processing in the sense provided for in article 91 of the Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights (hereinafter referred to as LOPDGDD).

Another recommended measure is that the collection of data is carried out consciously by the individual, and even with the requirement of a positive action to initiate the processing of biometric data, which, as indicated, would imply that the affected person has prior and sufficient information to be aware of the risk posed by the processing of their biometric data, especially if you are in a vulnerable situation.

The measures presented here are not exhaustive nor do they exhaust the set of measures that can or should be implemented to manage the risks that may arise from a specific implementation of the registration of working hours with biometric techniques. In addition, the validation of the biometric systems used in a processing must be ensured "by design" as required by art. 25(1) of the GDPR and with the recommendations established in the Guide to Privacy by Design.

C. PASSING THE ADEQUACY, NECESSITY AND PROPORTIONALITY ASSESSMENT

The GDPR requires in art. 35(7)(b) that, in a high-risk processing, prior to any implementation decision, the triple test of suitability, necessity and strict proportionality, also provided for by the doctrine of the Spanish Constitutional Court, must be passed.

With regard to the analysis of suitability and necessity, we refer to what is stated in Section V.A of this document in relation to both requirements. In order to establish the suitability of biometric processing, it is necessary to assess that there is a logical and direct link between the processing and the objective pursued, and to determine the real effectiveness of the processing, i.e., to determine by means of objective evidence that it is capable of achieving a minimum level of effectiveness in resolving the need raised.

As for passing the strictly necessity analysis, it must be demonstrated that it solves a problem that must be real, present or imminent, and critical to the functioning of the processing. In this regard, the ECtHR[17] established that "*necessary" "(...) it wasn't synonymous with indispensable (...) nor does it have the flexibility of expressions such as*

[17] Handyside v United Kingdom, Case No 5493/72 (ECtHR, 7 December 1976), paragraph 48.

'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'." Mere convenience or profitability[18] is not enough. In addition, the scope, extent and intensity of interference must be assessed in terms of impact on fundamental rights, explaining with evidence why other possible alternatives are not sufficient to meet this need sufficiently. Even when evaluating options, consider the possibility of employing a combination of measures, both automated and non-automated, organizational, legal or technical.

In the case of the registration of working hours, the worker has the obligation to participate in the processing of the clocking in/out and there is no lifting of the prohibition based on articles 9(2)(b) to 9(2)(g). Therefore, if the additional processing of biometric data is intended to be based on consent, it must be free, in order for it to be free, the controller must have options equivalent to biometric processing. So, if those equivalent options exist, biometric processing is not necessary. Therefore, a processing of clocking in/out implemented with biometric techniques, and which lifts the prohibition of Art. 9(1) GDPR based on the free consent of the data subject, does not pass a necessity assessment in the context of a DPIA.

With regard to passing the assessment of proportionality in the strict sense, it is necessary to establish whether the processing of biometric data is a weighted or balanced measure, since it derives more benefits or advantages for the general interest than harm to other goods or values in conflict. To this end, an assessment must be made of the level of intrusion into the rights and freedoms of the data subject. It should assess , among others: the nature of the interference: or how rights and freedoms are limited or put at risk; the scope/extent of the processing; the context in which the measure is to be applied or the nature of the activity that is the subject of the measure; whether "collateral intrusions" may occur, including interference with the privacy of persons other than the subjects directly affected by the measure.

In this regard, Opinion 3/2012 of the Article 29 Working Party on the Evolution of Biometric Technologies states that the loss of privacy must be objectively weighed against the expected benefits. In particular, the **fact that biometric processing entails savings that are not significant is not sufficient justification** for carrying out the processing.

> *"When analysing the proportionality of a proposed biometric system... A third aspect to consider is whether the resulting loss of intimacy is proportional to the expected benefits. If the benefit is relatively minor, such as increased comfort or slight savings, then loss of privacy is not appropriate."*

D. IMPLEMENTATION

There is a big difference between the concept of biometric operation and its implementation. Actual implementations involve the selection of sensors, communication protocols, development libraries, devices on which they are integrated (e.g., mobile phones or ATMs), storage (e.g., in the cloud), etc. Each of them will have different degrees of quality, certification, audit, security, third-party involvement, etc.

In the specific implementation of a clocking and attendance control processing with biometric techniques, additional data protection risks may arise, in addition to potential breaches, and international data transfers without adequate guarantees. Even if these situations had been initially resolved, they could rise as a result of a renewal or upgrade of its components once the system had been put into production.

[18] Article 29 Working Party, Opinion 3/2012 on developments in Biometric Technologies, WP 193, 27.04.2012, p. 8.

E. CONTEXT OF PROCESSING

In relation to the above, just as the biometric operation must be evaluated within the framework of the processing, the entire processing as a whole must be evaluated taking into account the social context and the collateral and unforeseen effects on the rights and freedoms that, by incorporating biometric operations, have occurred or are occurring in the environment (diversion of purposes, social impacts, regulatory changes, religious or cultural changes, conflicts, etc.).

F. MINIMUM DEFAULT MEASURES

In addition to a legal basis for the processing of Art. 6(1) of the GDPR, a circumstance that lifts the prohibition on processing special categories of data (Art. 9(2) of the GDPR), and compliance with the conditions of Art. 22 GDPR, it is necessary to establish appropriate technical and organisational measures by design in order to guarantee and be able to demonstrate that the processing is in accordance with this Regulation. These measures, taking into account the nature, scope, context and purposes of the processing, must be appropriate to manage the risk (Articles 24 and 25(1) of the GDPR) and, regardless of the level of risk, must implement data protection by default (Art. 25(2) GDPR).

Among the minimum default measures, the Spanish Data Protection Agency, in the guide "Data Protection in Labour Relations", in the section "Biometric data" of chapter 4.6, has already established the following set of guarantees, which can be extended to all kind of attendance control processing:

- Inform subjects of data on biometric processing. This implies, as stated in recital 39 of the GDPR, that "*Natural persons must be aware of the risks*" in relation to processing, in this case biometrics.
- Implement in the biometric system the possibility of revoking the identity link between the biometric template and the natural person.
- Implement technical means to ensure the impossibility of using the templates for any other purpose.
- Use encryption to protect the confidentiality, availability, and integrity of the biometric template.
- Use specific data formats or technologies that make it impossible to interconnect biometric databases and disclose unverified data.
- Delete biometric data when they are not linked to the purpose for which they were processed.
- Implement data protection by design.
- Carry out a Data Protection Impact Assessment prior to the start of the processing.

All these requirements are necessary, but not sufficient, conditions that must be implemented, objectively assessed and documented, in order for access control based on biometric processes to comply with the requirements of proportionality of processing.

G. PERSONAL DATA BREACHES

The reality of technology is that new ways to exploit security vulnerabilities appear every day, technical or social engineering. Within the framework of the processing where the biometric operation is located, the controller has to consider possible scenarios of personal data breaches, in order to, as a result of its analysis, implement guarantees to minimize not only the probability of their occurrence, but also to minimize the impact on the rights and freedoms of citizens in the event that they materialize.

In risk management, measures and guarantees must be determined to minimize the impact that the use of biometric systems may have on the rights and freedoms of data subjects, assuming that it is inevitable that a personal data breach will happen.

The scenarios that should be considered are, at least, the filtering or loss of biometric patterns, malicious use of stored patterns, intrusion into the biometric analysis system and its results, interception of communication between systems, denial-of-service attacks, discontinuity of own or third-party services, etc. All scenarios must be analysed to measure the degree of impact it may have on rights and freedoms.

Likewise, it is necessary to know what gaps are currently occurring and that could determine the inadequacy of a specific biometric technique, biometrics in general or the guarantees implemented. This involves carrying out a continuous evaluation of the processing according to the events that are taking place in the social and technological context.

IX. OUTSOURCING OF WORKERS

In the case of subcontracting of workers, if the contractor contractually requires biometric systems for the establishment of possible clocking in/out or attendance control, that requirement must comply with the provisions of this document.

The contracted company, if it also has the role of data processor, also has the obligation, as established in art. 28(3) GDPR: "*the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other data protection provisions of the Union or of the Member States*".

Therefore, if the conditions of compliance with the provisions of the GDPR are not met, the contracted company is not obliged to carry out the registration of working hours or access control in the workplace by implementing biometric techniques.

X. CONCLUSIONS

In relation to the processing of clocking and attendance control using biometric identification or authentication techniques, data controllers must take into account that:

- The use of biometric identification and authentication technologies in clocking and attendance control process involves high-risk processing that includes special categories of data.
- In the implementation of clocking and attendance control processing, the principles of data minimization and data protection by design and by default must be complied, using equivalent alternative measures, less intrusive, and that process the minimum additional data.
- There must be a circumstance to lift the prohibition on processing special categories of data and, in addition, a condition that legitimises the processing.
    - In the case of recording working hours and attendance control for work purposes, if the lifting of the prohibition is based on Art. 9(2)(b), the controller must have a regulation with the force of law that specifies the possibility of using biometric data for this purpose, which is not found in the current Spanish legal regulations.
    - In the case of recording working hours or attendance control in the workplace, consent cannot lift the prohibition of processing, nor be a basis for determining lawfulness, as there is generally a situation of imbalance between the data subject and the data controller.

  - In the case of attendance control outside the workplace, the performance of a contract is not a circumstance that lifts the prohibition according to Art.9(2) of the GDPR. Consent cannot be either, as it is a high-risk processing, and would have to exceed the requirement of necessity established for such processing.
- Any use of biometric data for additional purposes other than clocking and attendance control must have its own circumstances for lifting the prohibition and conditions that legitimise it.
- In the processing of clocking and attendance control, automated decisions that have legal effects on the data subject or similarly significantly affect him or her based on the biometric process cannot be made without human intervention, if the proportional circumstance to the objective pursued of an essential public interest based on a rule having the force of law is not met, to respect the essence of the right to data protection and to establish appropriate and specific measures to protect the interests and fundamental rights of the data subject.
- In the event that the biometric system is implemented with artificial intelligence techniques, in order to include them in a processing, the prohibitions, limitations and requirements established in the artificial intelligence regulations must be taken into account.
- In any case, it will be mandatory to pass, prior to the start of the processing, a Data Protection Impact Assessment in which, among others, the accreditation of the passing of the triple analysis of suitability, necessity and proportionality of the processing of biometric data is documented.
- Once all the requirements for compliance with the general principles of the GDPR have been met, organisational, technical and legal guarantees must be implemented in the practical implementation of time and attendance control processing with biometric identification or authentication techniques. In particular, at least the following default measures should be present:
  - Inform workers, or people if they are not in a work environment, about biometric processing and the high risks associated with it.
  - Implement in the biometric system the possibility of revoking the identity link between the biometric template and the natural person.
  - Implement technical means to ensure the impossibility of using the templates for any other purpose.
  - Use encryption to protect the confidentiality, availability, and integrity of the biometric template.
  - Use specific data formats or technologies that make it impossible to interconnect biometric databases and disclose unverified data.
  - Delete biometric data when they are not linked to the purpose for which they were processed.
  - Apply minimization of the biometric data collected, with an objective assessment that there is no possibility of disclosing special categories of additional data.
  - In the case of time and attendance registration or access control in the workplace, the collective agreements must include the set of guarantees in relation to this processing in the sense provided for in article 91 of the LOPDGDD.
- Among the recommended measures to minimize the risk are:

  - The use of biometric technologies should be based on the use of devices under the exclusive control of the data subjects.
  - It is recommended that the data collection be carried out consciously by the individual, and even with the requirement of positive action to initiate the processing of biometric data.
  - Preferably, centralized storage of biometric templates should not be used.
  - Automated data suppression mechanisms should be implemented.
- Finally, all actions and measures implemented will be reviewed and updated when necessary.