SPAIN

Trends and Developments

Contributed by:
Agustín Puente Escobar and Natalia González Vera
Broseta Abogados

Broseta Abogados was founded in 1975 and celebrates its 50-year trajectory this year. More than 300 professionals with deep technical expertise provide a full range of services and multidisciplinary advice. With a consolidated geographical presence in Spain, Portugal and Switzerland, this agile and flexible firm has a structure that allows it to adapt to the most complex environments with proactivity and to react to any contingency with the efficiency that the market and the clients demand. The firm's team of partners head up all its projects – professionals with an average of 30 years of experience, who are accessible, proactive and involved in every decision that affects the client. Broseta Abogados promotes transformation as the basis for growth, rejecting static and standardised solutions. Each client is viewed as a welcome challenge and their needs define the firm's service proposal. The team aims to enhance each client's value based on a differentiated way of doing things.

Authors

Agustín Puente Escobar is a partner in Broseta Abogados' privacy, IT and digital environments department. Agustin has been a state lawyer since 1994 and was chief of the Spanish Data Protection Agency (AEPD)'s legal cabinet from 1999 to 2018. Among Agustín's most notable works at the AEPD were his participation in the negotiations of the General Data Protection Regulation and the drafting of the Spanish Data Protection Act. Agustín has been honoured with several distinctions and recognitions from both the public sector and the private sector. He is considered one of the best in the practice of privacy and data protection – ranked in Band 1 by Chambers & Partners.

Natalia González Vera is an associate in the IT, privacy and digital environments department at Broseta Abogados. She has a law degree from the Complutense University of Madrid and a master's degree in corporate law from the Garrigues Study Centre. Natalia is currently working as a privacy specialist lawyer and has eight years of experience – focused mainly on providing specialised advice on projects with personal data protection and privacy law implications to national and international companies developing their activities in the most significant economic sectors. She has additional has experience in the areas of e-commerce and IT.

Contributed by: Agustín Puente Escobar and Natalia González Vera, **Broseta Abogados**

Broseta Abogados

Paseo de la Habana 101
Madrid 28036
Spain

Tel: +34 914 323 144
Email: info@broseta.com
Web: www.broseta.com

The Positions of the Spanish Data Protection Agency and the European Data Protection Board Regarding the Legal Grounds for Biometric Data Processing

In recent times, the use of biometric technologies has grown exponentially in a wide range of areas, including:

- identity verification for access control, especially in sectors such as sports, gambling venues, or environments requiring a specific level of security;
- workplace access control for employees and visitors; or
- the authentication of data subjects in certain online services or applications (eg, banking apps or even for unlocking mobile devices).

Alongside this growth, data protection authorities have also increased their concern about the processing of these categories of data – given that, by referring to unique and immutable characteristics of individuals, such categories of data can pose significant risks in the event of their misuse by third parties. Based on the various documents adopted by a multitude of authorities and organisations, these risks can be summarised as follows.

- Immutability of the biometric vector – unlike other authentication methods, biometric templates cannot be modified or revoked throughout the life of the data subject.
- Reversibility of the biometric vector – it is possible to reconstruct the original biometric information from stored templates, when they represent specific and characteristic points of the element from which the biometric data is extracted. In this way, in the event of an attack on a centralised base, it would be possible to rebuild the model from which that template was generated.
- Interoperability of biometric recognition systems – once the biometric templates are created, they could be reused in different systems for multiple purposes.

On the other hand, biometric data processing is not only governed by the EU's General Data Protection Regulation (GDPR), but also by the Artificial Intelligence Regulation (IAR), which classifies such processing into three categories:

- generally prohibited processing activities;
- high-risk activities; and
- activities not included in the previous categories.

This regulatory impact is driven by advancements in biometric recognition technologies. Traditional systems-based biometrics patterns and distance measurements between data

points (landmarks system) are now being supplemented by AI-based models, such as renewable biometric references (RBR), which may mitigate the aforementioned risks.

Based on these premises, several recent decisions have established highly restrictive criteria regarding biometric data processing – although the degree of restriction varies.

Given the brevity of this article, it will focus on the position adopted by the Spanish Data Protection Agency (*Agencia Española de Protección de Datos*, or AEPD) and the European Data Protection Board (EDPB), which have examined the issue in greater detail. However, other data protection authorities have also addressed this matter.

As a preliminary consideration, biometric data falls within the special categories of personal data outlined in Article 9(1) of the GDPR. Therefore, its lawful processing requires:

- the application of an exception to the general prohibition under Article 9(2) of the GDPR;
- the existence of a valid legal basis under Article 6(1) of the GDPR; and
- compliance with the remaining data protection principles set forth in Article 5(1) of the GDPR.

Evolution of AEPD criteria

Until the adoption of its "Guide to Attendance Monitoring Using Biometric Systems" ("the Guide"), the AEPD had been establishing in its different opinions and resolutions uniform criteria in relation to biometric data processing (essentially focused on facial recognition), based on the following elements.

- As the joint application of Articles 9(2) and 6(1) of the GDPR is necessary, the only possible legal bases for the processing would be – in general – that the processing was necessary for the performance of a mission in public interest or that the data subject has given their consent to the processing.
- For processing based on public interest, processing must be explicitly recognised in a legal provision that should also establish minimum safeguards, including specifying the type of biometric data to be processed.
- For consent to be lawful, it must meet the requirements set out in the GDPR (in particular, the condition that it be freely given), ensuring that data subjects have an alternative that does not involve biometric data processing.
- In all cases, processing must be proportionate to its intended purpose.

Applying these criteria, the AEPD:

- imposed a significant fine on a supermarket chain for attempting to use facial recognition on all its customers to prevent access by prohibited individuals;
- ruled that a bank's facial recognition system for AML compliance violated the GDPR;
- determined that facial recognition for online university exams was permissible only if students could opt to take exams in person; and
- found that biometric access control for sports venues could not be based on sport violence prevention laws (which did not regulate it) and could only be implemented with freely given consent and an alternative method.

However, in November 2023, the AEPD modified these criteria with the adoption of the Guide, which states that it is adopted with the objective of "determining the criteria for the processing of

attendance monitoring using biometric systems in accordance with the GDPR" – whether for working or non-working purposes – and identifies the measures that must be adopted for the processing to be considered compliant with the GDPR and other applicable rules.

The Guide indicates as a first consideration that "the different products available on the market for the collection of biometric data that record such data with a precision, detail or frequency that is well above the needs of a specific processing violate the principle of minimisation". The Guide considers it necessary that the solution chosen for the processing of data is respectful of this principle and is configured in such a way as to avoid the collection of biometric data where it is unnecessary.

Likewise, the Guide – following the EDPB criteria – provides that biometric data processing always involves special categories of personal data, regardless of whether the data is used for identify the data subject within a specific universe (1:N comparison) or only to authenticate them (1:1 comparison). It thus revises its previous stance that only identification processing falls into this category.

Sections V and VI of the Guide analyse the possible legal grounds for the processing, focusing on the possibility that the processing may be based on the exceptions set out in Article 9(2)(a) and (b) of the GDPR – ie, that:

- the data subject has given their explicit consent to the processing, which is not prohibited by domestic law; and
- "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 EU 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".

The Guide does not analyse the possible legal basis of the public interest, on which it had already ruled in the past.

Regarding the applicability of Article 9(2)(b), the AEPD indicates that processing will only be possible when a regulation with the force of law or a collective agreement incorporates a sufficiently specific authorisation indicating that the processing is necessary for the fulfilment of the purposes that justify it, justifying that need and establishing the measures that must be adopted for the processing to be lawful.

On the other hand, with regard to the exception contained in Article 9(2)(a) of the GDPR and after ruling out its applicability in the workplace as a result of the "imbalance of power" existing in labour relations, the Guide applies the principles of freedom of consent and the necessity of processing to reach a conclusion that de facto prohibits the processing of biometric data based on the consent of the data subject. The Guide's reasoning is summarised as follows: given that biometric data processing is more intrusive than other data processing that does not involve special categories of data and that, in order for the processing of biometric data to be based on the consent of the data subject, the existence of an alternative means that enables the same purpose and does not entail such processing is necessary (as, otherwise, the consent would not be free), the logical consequence will be that the processing of biometric data is not necessary – in the sense of being essential to achieve the aim

pursued – and so the processing of biometric data can never be based on consent.

This de facto prohibition involves a modification of the rule provided for in Article 9.1 of Organic Law 3/2018, which adapts Spanish law to the GDPR. Article 9.1 establishes that "[f]or the purposes of Article 9(2)(a) of Regulation (EU) 2016/679, in order to avoid discriminatory situations, the consent of the data subject alone will not be sufficient to lift the prohibition on the processing of data whose main purpose is to identify their ideology, trade union membership, religion, sexual orientation, beliefs or racial or ethnic origin", excluding health, biometric and genetic data from this prohibition.

The AEPD has applied the content of the Guide in several resolutions. Thus, in May 2024, it fined a gym in which a mandatory biometric access control had been established EUR27,000. Likewise, in December 2024, the AEPD sanctioned a public law corporation that established access control in the workplace by means of the digital fingerprint – albeit without a financial fine, as the exception of Article 83.7 of the GDPR applies in Spain. However, the main resolutions adopted have affected football clubs that had established biometric recognition systems based on the consent of the data subject for access to their stadiums.

However, the scope of these resolutions is different. Thus, until December 2024, the AEPD sanctioned an alleged breach of Article 9(1) of the GDPR on the grounds that the principle of lawfulness and the prohibition of processing special categories of data had been violated. Likewise, in cases where the processing was based on consent, applying the reasoning contained in the Guide, the AEPD also sanctioned the violation of the principle of data minimisation – considering that the processing was not necessary, as it was possible to achieve the purpose pursued by it without the processing of biometric data. However, in the last of the published decisions (that of procedure PS/00482/2023), the AEPD only found that the principle of data minimisation had been infringed and not Article 9(1) of the GDPR – considering that, once the first of the infringements has been declared, it is unnecessary to assess whether the consent is valid.

In summary, the AEPD appears to interpret that – unless there is an express authorisation for the processing of biometric data in a legal provision, which also establishes the guarantees that must be adopted – the processing will be deemed contrary to the GDPR. However, in its most recent resolutions, the AEPD has opted to consider only the violation of the principle of data minimisation, without assessing the validity of the consent provided (where appropriate) by data subjects – although it implicitly deems such consent to be contrary to the GDPR.

EDPB criteria

The processing of biometric data has also been subject to assessment by the EDPB, as it was by the Article 29 Working Party. Thus, it is worth referring to – among others – the Working Document on Biometrics adopted in August 2023 or to Opinion 3/2012 on Developments in Biometric Technologies of April 2012.

Likewise, after the full application of the GDPR, reference should be made to Guidelines 3/2019 on processing of personal data through video devices (adopted in January 2020) and Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (adopted in April 2023), as well as – in particular – to the more recent Opinion 11/2024 on the use of facial recognition to streamline airport pas-

sengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 of the GDPR).

Regarding the legal base for the processing, paragraph 77 of Guidelines 3/2019 provides that "[t]he use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (eg, marketing, statistical, or even security) will, in most cases, require explicit consent from all data subjects (Article 9(2)(a))", including – as an example – the case where, "[t]o improve its service, a private company replaces passenger identification checkpoints within an airport (luggage drop-off, boarding) with video surveillance systems that use facial recognition techniques to verify the identity of the passengers that have chosen to consent to such a procedure". In this case, the above-mentioned Guidelines explain that the processing would be lawful, provided that "passengers – who will have previously given their explicit and informed consent – enlist themselves at, for example, an automatic terminal in order to create and register their facial template associated with their boarding pass and identity" and that the checkpoints with facial recognition are "clearly separated", so that "[o]nly the passengers, who will have previously given their consent and proceeded with their enrolment, will use the gantry equipped with the biometric system".

Subsequently, Opinion 11/2024 analyses this issue – albeit with a different approach to that of Guidelines 3/2019, given that:

- it does not refer to systems established by entities operating at the airport but, rather, to the flow of passengers at airport controls in which the identification of the data subject is mandatory; and
- it analyses its compatibility with Articles 5 (1) (e) and (f), 25 and 32 of the GDPR and not the legal basis for the processing – although it contains some assessments in this regard in paragraph 15, indicating that:
  - (a) individuals would need to be able to easily withdraw such consent at any time and without any detriment;
  - (b) individuals should be able to freely choose whether or not to use these services and without any detriment, incentives, additional costs or additional advantages in return;
  - (c) individuals who did not explicitly consent to facial recognition for the purpose intended would not have their faces scanned by cameras; and
  - (d) the principles of processing enshrined in Article 5 of the GDPR with regard to necessity and proportionality still apply, even when individuals have provided their explicit consent to the use of their biometric data.

Opinion 11/2024 analyses various scenarios related to the specific processing of biometric data, including:

- when the biometric template is only in the possession of the data subject themselves (for example, by means of a QR in an app or other device on their mobile terminal that is shown to the reader together with their face or fingerprint) so that the process would be authentication (1:1);
- when the template is stored encrypted on the controller's servers, located in the same space where the identification is carried out, with the decryption key in the possession of the data subjects; and
- when the circumstances of the previous case are met but the decryption key is not in the

possession of the interested party but, rather, in the possession of the controller.

Opinion 11/2024 considers that, in the first two scenarios and provided that measures are adopted to strengthen the security of the processing and the rights of the data subjects, the processing could be in accordance with Articles 5(1)(f), 25 and 32 of the GDPR.

As regards the principle of data minimisation, Opinion 11/2024 indicates that the processing would be necessary if "the controller can demonstrate that there are no less intrusive alternative solutions that could achieve the same objective as effectively" – for example, if it can be demonstrated that the processing "speeds up the verification process compared to the current situation, which includes a human checking whether the name on the boarding pass matches the passenger's identity document".

Therefore, the system based on consent would be lawful if:

- the identification of the data subjects was already being carried out and was necessary or legally required;
- the recognition system is complemented by an element (the facial template or decryption key) in the possession of the data subject; and
- it has been demonstrated that the system allows the access process to be streamlined with regard to procedures based on identification by staff.

Executive conclusions

There is a clear discrepancy between the criteria of the EDPB and the AEPD, given that – whereas the latter seems to limit the processing almost to the point of prohibition – the former admits it under certain safeguards.

The main discrepancy is in the assessment of the need for processing, which – in the case of the AEPD – is applied to the ultimate purpose (access), without taking into account other elements such as agility of access, which the EDPB does consider. And this affects the admissibility of consent as a legal basis for processing.

On the other hand, there is no doubt that the controller will have to carry out a thorough analysis of the conditions of the processing in order to minimise the risks to the rights and freedoms of individuals, while also reinforcing the security of the processing.

However, it is important to bear in mind that both the criteria of the AEPD and the EDPB are based on a vision based on facial recognition systems that are now outdated (based on landmarks) and do not consider the existence of systems that mitigate the risks of immutability, reversibility and interoperability of biometric templates, such as those based on AI (eg, those based on RBR). For this reason, it seems logical that these criteria need to be updated in the short term, in order to adapt to technological developments in this area.

In addition, it will be essential to promote research into privacy protection techniques (eg, revocable biometrics or advanced anonymization) to minimise the security risks associated with the storage and processing of biometric personal data.