ECIJA
Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

# AEPD Report 2021/0047 on the treatment of biometric data in video identification processes in relation to Money Laundering Prevention.

**July 2021**

The AEPD has recently published a Legal Report analyzing a *project* which, in the words of the AEPD, "*considers the viability of processing biometric data for facial recognition at the time of customer registration at the office or through an online channel, in order to verify their identity and thus conduct the appropriate controls provided for in Law 10/2010, of April 28, 2010, on the prevention of money laundering and terrorist financing (AML/CFT), as well as fraud control*". In particular, the consultation and the report address the legal bases of legitimacy that would be valid, in the opinion of the AEPD, and specifically on the use of consent and / or public interest as an authorization for the processing described.

By means of this information note, ECIJA analyzes the interpretation of the AEPD and the impact that this Report may have on compliance with the duty of due diligence in the compulsory identification processes regarding money laundering prevention and in other areas, such as the issuing of qualified electronic certificates through video identification, among others.

It should be noted that the AEPD does not reproduce the content of the consultation it resolves, so many doubts arise as to the particular case on which the Report is based and, consequently, to what extent its conclusions can be extrapolated to other similar cases.

Perhaps this lack of detailed knowledge of the case is the reason behind the initial and surprising conclusion of this report, which **rules out the possibility of basing the processing of biometric data on the duly informed prior consent of the data subjects**, because, according to the AEPD, "*since we are dealing with biometric data, i.e. special categories of data, it cannot be an adequate legal basis as it depends on the clients' authorization for such processing. Furthermore, it can be considered that a mandatory consent would not be lawful, by conditioning the provision of services to the granting of consent, with the consequence that such consent would not be free*".

In general, consent is one of the legal bases included in Article 9 of the GDPR that allows the processing of special categories of personal data and the reason why its use is not applicable is not explained and, in particular, which circumstances are met to consider that it is not valid, in absolute terms, for this type of processing.

Applying the general contract theory and the general principles applicable to consent, the reality is that the AEPD seems to question the legality of the use of consent on the grounds that, in the case in question, there is no alternative for those users who do not wish to give their consent for this type of processing, thus preventing access to the financial services in question, which would undoubtedly invalidate the consent given, it being understood that if there were

an alternative for those users who decide not to give their consent, it would be a processing that could be covered by duly informed consent.

It is precisely this essential information that accompanies consent what seems to be decisive in the processing of biometric or especially sensitive data, in fact, it is decisive in all processing of personal data, to the extent that what is really relevant in the general theory of obligations and contracts is not so much the form or means through which consent is given, but that the prior information and the conditions under which it is given ensure that it is not vitiated. This is precisely the determining factor, in most cases, for being able to establish whether or not the consent is vitiated, and this seems to be the understanding of the General Regulation on Personal Data Protection, as it considers the autonomy of the will, provided that it is given with sufficient and transparent prior information, as well as the appropriate circumstances.

In addition, it is anticipated that biometric data will be considered a special category, with the AEPD returning to the theory that it made public months ago in relation to the differentiation between two determining concepts: **authentication** and **identification.**

a) **Authentication:** process in which the identity of a user is authenticated using the user's biometric data to compare them against another source provided by the same user, considered as a template or comparison document (for example, comparison of facial biometric data with the photograph of the ID card or passport provided by the same user). This is what is known as a "one-to-one" (1-to-1) authentication process.

b) **Identification:** process in which the identification of a user is carried out using the user's biometric data to compare them with a multitude of biometric patterns of multiple individuals, stored in one or multiple databases, being, therefore, a massive processing of biometric personal data (for example, comparison of the facial biometric data of an individual with a database in which there are thousands of biometric patterns obtained from other people). This is what is known as a "one-to-many" (1-to-N) authentication process.

In particular, for the case raised in the consultation analyzed by the AEPD, it is considered that it falls within the second case, a process of identification itself (one to many, 1-to-N), and therefore it is a process of identification, having the consideration of special category of data involving biometric data.

However, once again, since the content and scope of the project in question have not been clarified, there is no explanation as to why the process carried out is classified as identification and not authentication.

In principle, the logical reasoning, and following the AEPD's own criteria, it seems that it understands that the tasks pursued by the financial institutions lie in complying with the due diligence obligations in the identification processes regarding the Prevention of Money Laundering and Terrorist Financing (PBCFT) and the prevention of fraud, which, let us not forget, is nothing more than the prevention of the commission of crimes established by the Penal Code (for which it is necessary to carry out an adequate identification according to the existing state of the art at the specific moment, being the use of inherent factors -such as biometrics- the most effective for the prevention of the commission of such crimes), as long as they are

authentication processes (1-to-1) and not identification processes (at least not with the criteria established by the AEPD), they would still be perfectly valid processes.

As in the case of consent, and in relation to the processing of biometric data for identification processes (1-to-N), the AEPD denies the possibility of covering this processing on the basis of the existence of a public interest.

After a long legal reasoning in which the AEPD conditions the existence of this interest on it being expressly recognized in a regulation with the rank of Law that specifically defines the limits to the right to the protection of personal data, it considers that this interest does not exist in relation to what is regulated in the PBCFT law "*since the legislator has not foreseen the use of biometric data as a proportional measure for the identification of natural persons, establishing the specific and adequate guarantees that derive from the greater risks involved in the processing of such data*".

Consequently, the AEPD only considers it proportional to carry out an authentication process (according to the concept indicated above), in which the identity is verified by means of the reliable documents and the face of the individual in question who provides them, seeming to ignore in this assessment the measures and controls required in the different Instructions published by SEPBLAC to carry out the assisted and unassisted video-identification processes, in which it expressly refers to the responsibility of the obliged subject in relation to the implementation of "*the technical requirements that allow verifying the authenticity, validity and integrity of the identification documents used and the correspondence of the holder of the document with the customer being video-identified*".

In particular, the referred instructions issued in 2016 and 2017 by the Money Laundering Prevention Service (SEPBLAC) and duly justified under the provisions of Article 21.1d) of Royal Decree 304/2014, of May 5, approving the Regulation of Law 10/2010, of April 28, on the Prevention of Money Laundering and Terrorist Financing (RPBCFT), provide that it will be possible to perform the identification of the client in a non-face-to-face manner, complying with the duty of due diligence, provided that "*The identity of the client is accredited by means of the use of other secure client identification procedures in non-face-to-face operations, **provided that such procedures have been previously authorized by the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offenses***".

It is surprising that this legal provision and the aforementioned SEPBLAC instructions are not even taken into consideration when analyzing the possibility of using biometrics in the processes of authentication and/or non-face-to-face identification, which although not expressly mentioned in the regulation is, de facto, the only viable technology available now-a-days to allow secure identification, other than that expressly regulated in the aforementioned article 21 (qualified electronic signature, intervention of a notary public or pre-existence of an open account in a country with sufficient guarantees).

We are certain that SEPBLAC would have been very interested to know, prior to the publication of the aforementioned report issued by the AEPD, its conclusions regarding secure and robust identification processes, which for many years have allowed to reduce, by far, the number of fraudulent operations related to money laundering and terrorist financing, as well as the fight against organized criminal organizations specialized in the commission of financial frauds.

In this regard, it should be noted that, in relation to the identification in certificate issuance processes under Regulation (EU) n.No. 910/2014 (e-IDAS) and its implementing regulations, the recent approval of the Ministerial Order ETD/465/2021 "on non-presential identification methods for the issuance of qualified electronic certificate", issued on May 6, 2021 by the Ministry of Economic Affairs and Digital Transformation and the subsequent approval of the certification and compliance audit scheme published by the National Cryptologic Center, makes specific reference to the use of inherent factors to give compliance and provide the highest degree of security to the non-presential identification processes for the issuance of qualified electronic certificates.

However, in this Report, the AEPD concludes that the processing cannot be legitimized, neither in the customer's consent, nor in the alleged public interest, expressly stating that "*the DNI (ID) alone and for all purposes accredits the identity and personal data of its holder. Thus, imposing identification through facial recognition as mandatory would not be in accordance with the provisions of current regulations, in addition to being disproportionate, etc.*", without assessing whether it could be feasible, as it is expressly covered by the provisions of the GDPR, in the legitimate interest of the fight and prevention of fraud or in mere regulatory compliance, referring to all the regulations previously referred to in terms of PBCFT.

The content, interpretations and conclusions of the AEPD Report are far distant from the operational, technological and regulatory reality implemented to comply with the legal requirements established in the field of identification for the prevention of fraud and money laundering, specifically with respect to the identification processes carried out remotely, in which the establishment of measures that allow the verification of the reliable identification document used corresponds unequivocally to the subject (individual holder) who is carrying out the identification process is essential to reduce the risks of identity theft. Otherwise, it would not be possible to execute the said verification, giving wings, without even taking it into account, to the organized mafias that day by day try to put in check all kinds of businesses, both in financial fields, as well as in telecommunications, energy and in general, all services of massive character that allow, by express request of their users in many cases, the possibility of carrying out non face-to-face contracting, for which prior identification is always required.

In this sense, and in relation to report 47/2021, on facial recognition for the identification of persons on the basis of the regulations on PBC that are the subject of this Note, it should be interpreted that it is not that such facial recognition cannot be carried out, but that the possibility of carrying it out will depend, to a large extent, on the free and express consent of the data subject, which goes through the offer to the data subject of alternative method for identification (preventing the consent from being vitiated). This aspect could easily be covered in office identification by means of recognized reliable supporting documents and verification of correspondence with the person holding it by the employee, but does not find the same support with respect to remote identifications, even if this technology has proven to be completely effective in reducing fraud and identity theft.

In addition, the AEPD does not seem to take into account either the importance of the homogenization of processes in the fulfillment of the legal obligations of the entities, or the coordination with other national regulatory bodies, regardless of the channel through which these are carried out, since they are the basis for the accreditation of the due diligence of the

responsible parties to requirements and requests from the different authorities, as well as from the users in the event of possible claims.

In view of the legal uncertainty generated by a report of this type, and taking into account the risk associated with the limitation that may arise in relation to the use of a technology that is destined to be a key factor in the fight against money laundering and terrorist financing, as well as against any type of fraud associated with identity theft, especially in remote transactions, we can only hope that the legislator will intervene as soon as possible to establish a legal framework with the rank of law that expressly regulates the possibility of using biometric technology. This, taking into consideration that it has been proven that the use of these systems helps to hinder the actions of those who seek to bypass security controls, without their use entailing the persistent threat of a potential sanction for non-compliance with other related regulations based on the disparate interpretations of the various control bodies.

We remain at your disposal for any questions you may have.

Best regards,

**ECIJA's Privacy and IT Compliance Area**
info@ecija.com
Telf: + 34 91.781.61.60