Biometric data: Risk and protection

apdcat

Autoritat Catalana de Protecció de Dades

Identification

There are three possible ways of proving one's identity:

Using something you have. This method is relatively easy to do, whether by using the key to one's vehicle, a document, a card, or a badge.

Utilizing something you know, a name, a secret, or a password.

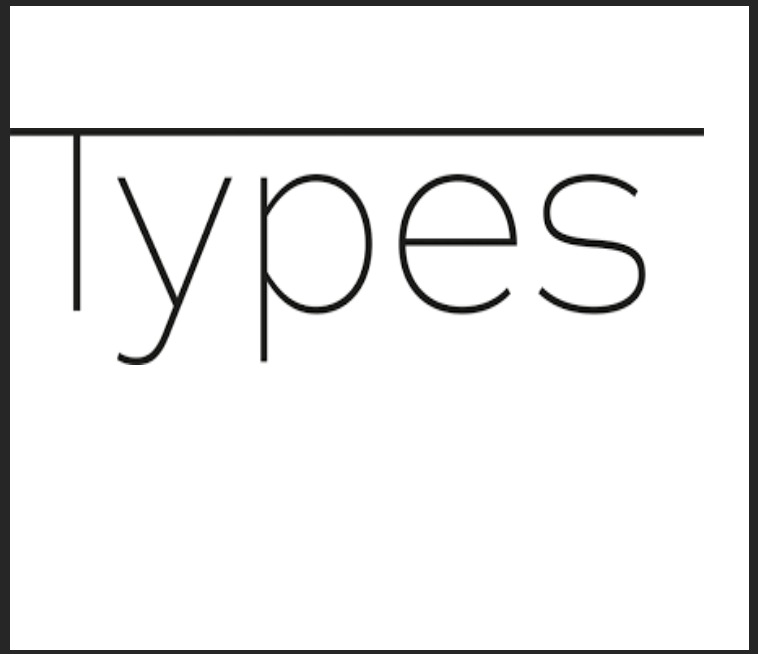
Through what you are, your fingerprint, your hand, your face.

Biometric data (GDPR)

Definition(s) Personal data resulting 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 dactyloscopic data.

While there are many types of biometrics for authentication, the five most common types of biometric identifiers are: fingerprints, facial, voice, iris, and palm or finger vein patterns.

Two types of biomètrics



Physiological measurements

They can be either morphological or biological.

Morphological identifiers mainly consist of fingerprints, the hand's shape, the finger vein pattern, the eye (iris and retina), and the face's shape.

Biological analyses, DNA, blood, saliva, or urine may be used by medical teams and police forensics

Behavioral measurements

The most common are: voice recognition, signature dynamics (speed of movement of pen, accelerations, pressure exerted, inclination), keystroke dynamics, the way we use objects, gait, the sound of steps, gestures, heartbeat, etc.

Identification & Authentication

Biometric authentication

Are you, indeed, Mr or Mrs X?"

Biometric identification

“Who are you?

TEMPLATE

USE CASES

Law enforcement and public security (criminal/suspect identification)

Military (enemy/ally identification)

Border, travel, and migration control(traveller/migrant/passenger identification)

Civil identification (citizen/resident/voter identification)

Healthcare and subsidies (patient/beneficiary/healthcare professional identification)

Physical and logical access (owner/user/employee/ contractor/partner identification)

Commercial applications (consumer/customer identification)

BE CONSCIOUS

Biometrics are not immune to data breaches.

If a malicious actor manages to get access to the database, then they get hold of your biometrics.

This not only is a risk to the business you're a part of, but it's also a risk to your identity as attackers can steal your biometrics for illegitimate purposes.

"You can not change your biometrical data"

LAWS

The Three Laws of Biometrics (Biometrics Institute)

1. POLICY – **comes first:** Any use of biometrics is proportionate, with basic human rights, ethics and privacy at its heart.

2. PROCESS – **follows policy:** Safeguards are in place to ensure decisions are rigorously reviewed, operations are fair and operators are accountable.

3. TECHNOLOGY – **guided by policy and process:** Know your algorithm, biometric system, data quality and operating environment and mitigate vulnerabilities, limitations and risks.

GDPR

Biometrics under the GDPR

The GDPR classifies biometric data as a type of special category of personal data. This means that you may not process biometric data. Even so, the GDPR allows you to process special categories of personal data if your processing falls within one of the lawful reasons for processing

Processing of special categories of personal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Exception

2. Paragraph 1 shall not apply if one of the following applies:
    1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
    2. 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 (…)
    3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
    4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it i(…)
    5. processing relates to personal data which are manifestly made public by the data subject;
    6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
    7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

Exception -2

8 . processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

SUITABLE RECITALS

(46) Vital Interests of the Data Subject

(51) Protecting Sensitive Personal Data

(52) Exceptions to the Prohibition on Processing Special Categories of Personal Data

(53) Processing of Sensitive Data in Health and Social Sector

(54) Processing of Sensitive Data in Public Health Sector

(55) Public Interest in Processing by Official Authorities for Objectives of Recognized Religious Communities

(56) Processing Personal Data on People's Political Opinions by Parties

LOPD

Article 9. Special categories of data.

1. For the purposes of article 9.2.a) of Regulation (EU) 2016/679, in order to avoid discriminatory situations, the sole consent of the affected party will not be sufficient to lift the prohibition on the processing of data whose main purpose is to identify their ideology, union membership, religion, sexual orientation, beliefs or racial or ethnic origin.

The provisions of the previous paragraph will not prevent the processing of said data under the protection of the remaining cases contemplated in article 9.2 of Regulation (EU) 2016/679, when applicable.

2. The data processing contemplated in letters g), h) and i) of article 9.2 of Regulation (EU) 2016/679 based on Spanish Law must be covered by a standard with the rank of law, which may establish additional relative requirements. to your security and confidentiality.

In particular, this rule may cover the processing of data in the field of health when required by the management of public and private health and social assistance systems and services, or the execution of an insurance contract of which the affected party be part.

Consent

Consent must be freely given, specific and informed indication of the data subject's wishes. (AAPP, employment)

It must be clear that such consent cannot be obtained freely through mandatory acceptance of general terms and conditions, or through opt-out possibilities. Furthermore, consent must be revocable. In this regard, in its opinion on the definition of consent, the Working Party underlines various important aspects of the notion: the validity of consent; the right of individuals to withdraw their consent; consent given before the beginning of the processing; requirements regarding the quality and the accessibility of the information .

In many cases in which biometric data are processed, without a valid alternative like a password or a swipe card, the consent could not be considered as freely given. For instance, a system that would discourage data subjects from using it (e.g. too much time wasted for the user or too complicated) could not be considered as a valid alternative and then would not lead to a valid consent.

Contract

Processing of biometric data can be necessary for the performance of a contract to which the data subject is party or can be necessary in order to take steps at the request of the data subject prior to entering into a contract. It has however to be noted that this applies in general only when pure biometric services are provided. This legal basis cannot be used to legitimate a secondary service that consists in enrolling a person into a biometric system. If such a service can be separated from the main service the contract for the main service cannot legitimate the processing of biometric data. Personal data are not goods that can be asked for in exchange of a service, therefore contracts that foresee that or contracts that offer a service only under the condition that someone consents to the processing of his biometric data for another service cannot serve as legal basis for that processing.

Substancial public interest

If you rely on a condition that requires you to demonstrate that your processing is necessary for reasons of substantial public interest, you **must** make sure the "public interest" is real and of substance. It is not enough for you to make a vague or generic public interest argument to support your purpose. You **must** make a specific argument about the concrete wider benefits of your processing. This is due to the sensitive nature of processing biometric data to uniquely identify people.

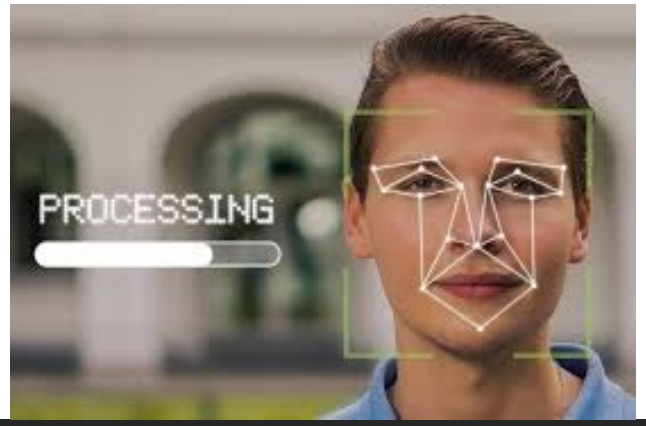
LEGAL BASIS (STC 76/2019)

LAW RESERVATION:

CLEAR

CONCRETE

PREDICTABLE



Examples

Case by case

apdcat

Autoritat Catalana de Protecció de Dades