ONTIER

15th November 2016
#3

Index

EXTENSION OF SENSITIVE DATA: GENETIC AND BIOMETRIC DATA

The GDPR extends the scope of sensitive data to include genetic and biometric data. Generally, the processing of sensitive data requires explicit consent from the data subject. Furthermore, if the processing is being carried out on a large scale it also requires the completion of privacy impact assessments and the designation of a Data Protection Officer, among other requirements.

Current situation

Directive 95/46/EC lists certain types of data that are highly sensitive in nature and closely related to fundamental rights, particularly the right to privacy. Article 8 defines sensitive data as that which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning health, sex life or sexual orientation. The processing of sensitive data is only lawful when the data subject has explicitly consented to it. However, EU Member States may determine cases where not even the data subject can authorise the processing of sensitive data. In Spain, for example, Article 7.4 of Law 15/1999 on the protection of personal data forbids the creation of files whose sole purpose is to store sensitive data.
According to Directive 95/46/EC, it is sometimes possible to process sensitive data without consent. For example, when the data is necessary for employment issues, when it is necessary to safeguard a vital interest of the data subject, or when the processing is carried out by a political party or other non-profit entity.

What's new?

Article 9 of the GDPR updates the category of sensitive data to now include genetic and biometric data. Both are defined in Article 4 of the GDPR; Genetic data is defined as 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that person.' Recital 34 specifies that genetic data is derived from chromosomal, DNA or RNA analysis, although this is not an exhaustive list. Biometric data is defined as '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 person, such as facial images or fingerprints.'
The inclusion of genetic data as sensitive data particularly affects the health sector in the context of clinical analysis. The inclusion of biometric data as sensitive data will affect almost every company that operates in the information society. This is due to their use of authentication mechanisms based on biometric data to identify their clients or users, as these mechanisms are the only method of ensuring that a client or user is who they claim to be. In fact, some companies already control access to private userspaces via fingerprint or by capturing a simple selfie.
The GDPR maintains the obligation to obtain explicit consent in order to process sensitive data, as long as there is the possibility to ignore consent, such as in the following cases:

- When the processing is necessary to comply with employment or social security obligations, provided that it is authorised by EU law, Member State law or a collective agreement.
- When the processing is necessary to protect the life of the data subject, who is not physically or legally capable of giving consent.
- When the processing is carried out by a foundation, association, political party or other non-profit entity with regard to the data of its members.
- When the data subject has made this personal data available to the public.
- When processing is necessary to file a claim or defence in court.
- When the processing is necessary for reasons of public interest, given certain conditions.

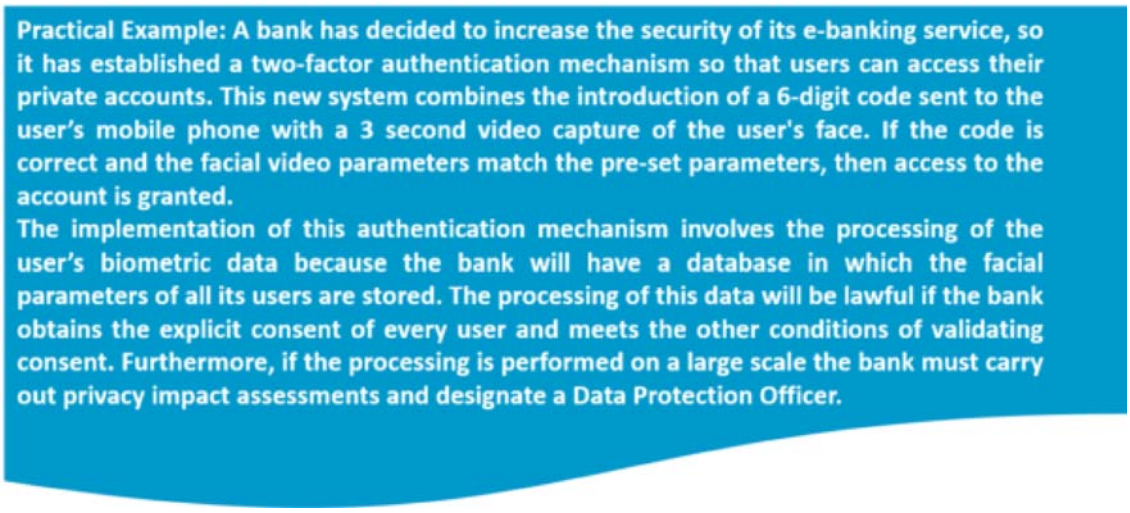
- When the processing is necessary for the purposes of preventive or occupational medicine.
- When the processing is necessary for archive, scientific or historic research or statistical purposes.

Member States may also establish additional conditions or limitations on the processing of certain types of sensitive data, such as health data, genetic data and biometric data. However, according to Recital 53 of the GDPR, these specifications cannot become an obstacle to cross-border data processing.

Finally, the company that processes sensitive data on a large scale, including genetic or biometric data, shall (i) carry out privacy impact assessments and (ii) designate a Data Protection Officer in accordance with articles 35 and 37 of the GDPR.

What to do to adapt?

Companies that process a person's genetic or biometric data must obtain their explicit consent and meet the other conditions set out in Article 7 of the GDPR. They must store the information using appropriate security measures according to the sensitivity of the particular data, as well as carry out privacy impact assessments and designate an (in-house or external) Data Protection Officer. They must also be aware of any further limitations that may be introduced by each Member State on the grounds set out in the GDPR.



Practical Example: A bank has decided to increase the security of its e-banking service, so it has established a two-factor authentication mechanism so that users can access their private accounts. This new system combines the introduction of a 6-digit code sent to the user's mobile phone with a 3 second video capture of the user's face. If the code is correct and the facial video parameters match the pre-set parameters, then access to the account is granted.
The implementation of this authentication mechanism involves the processing of the user's biometric data because the bank will have a database in which the facial parameters of all its users are stored. The processing of this data will be lawful if the bank obtains the explicit consent of every user and meets the other conditions of validating

consent. Furthermore, if the processing is performed on a large scale the bank must carry out privacy impact assessments and designate a Data Protection Officer.

TEAM

Joaquin Muñoz Rodríguez (Spain)
Pablo Uslé Presmanes (Spain)

Ana Rocha (Portugal)
Ana Festas Henriques (Portugal)

Derek Stinson (UK)
Paula Enríquez (UK)

Read more:

about us

Share on:

Subscribe:

our Newsletters

Contact us:

Website | LinkedIn

Rua Vitor Cordon Nº10A, 4º piso - 1249 - 202 Lisboa | Portugal
Tel. (+351) 213 223 590 / Fax (+351) 213 223 599

Rua Pedro Homem de Melo, n.º 55 - 8.º piso - 4150 - 599 Porto | Portugal
Tel. (+351) 223 190 888 / (+351) 220 924 945