POSITION PAPER

General ESBG considerations on the EDPB 3/2019 draft Guidelines on processing of personal data through video devices

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

[09.09.2019]

ESBG

- ESBG would like to raise concern on s**ection 5.1 on "general considerations when processing biometric data"**. In this section, we consider that the draft Guidelines adopt an approach that has confusing results with contradictory guidelines.

- **Guidelines 73 and 74** clearly express that "t*he video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual*" and that "*in order for it to be considered as processing of special categories of personal data (Article 9) it requires that biometric data is processed "for the purpose of uniquely identifying a natural person*". Hence it can be derived from the above that the capture of video footage cannot be considered as treatment of biometric data when the data captured on the video cannot uniquely identify an individual.

  However, **Guideline 76** goes on to say that "*The use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require explicit consent of all data subjects (Article 9 (2) (a)), however another suitable exception in Article 9 could also be applicable*". And provides an example of a controller that manages access to his building using a facial recognition method, the draft Guidelines also affirm that the facial recognition method should be triggered by the data subject himself, for instance by pushing a button.

  The following Guideline 78 rightfully treats the aspect of biometric templates, considering that all the intermediate templates made on the fly (with the explicit and informed consent of the data subject) in order to be compared to the ones created by the data subjects at the time of the enlistment, are immediately and securely deleted.

  But, as the example provided by the EDPB has some close similarities with how banks are aiming to (or some have already done so) implement facial recognition techniques at their physical branches, ESBG would like to raise some concerns on some issues.

  - ESBG considers that **the draft Guidelines are missing that when video footage is obtained by a controller, and some data subjects have previously given explicit and informed consent of that treatment, and have enlisted on a special registry with their biometric data, the data obtained from the video footage cannot, technically, be able to uniquely identify data subjects that have not been enlisted and that have not consented to include their biometric data on any registry.**

  - In relation to the example on the controller that manages access to his building using a facial recognition method, **ESBG is of the view that the method can only be beneficial both to the controller and to those who have enlisted to use their biometric data if the access is made more dynamic, innovative, and retains all security aspects.** Therefore, if those data subjects need to push a button and wait for the facial recognition method to work, the method will become less attractive for both sides and the innovation will not be positive.

  - In addition to that, **ESBG considers that a relevant technical aspect is missing in the analyses shown at the draft Guidelines.** In practice, facial recognition methods cannot uniquely identify a person if that person has not been previously enlisted in a registry, which would require an explicit consent. And that being the case, if both enlisted and non-enlisted individuals access a building and video footage is caught of them, non-enlisted ones will not be uniquely identified. It will be technically not possible.

As a consequence of the above considerations, **ESBG considers that the EDPB should take into account all the technical aspects of the processing of biometric data through video devices, and not hinder innovative solutions such as facial recognition methods. We are of the opinion that the examples provided in the draft Guidelines do not fully reflect the practical and technical aspects of video surveillance systems, and that they are not fully coherent with the approach expressed in guidelines 73 and 74.** This approach is also in line with the definition of "biometric data" in article 4(14) of the GDPR, and Recital 51.

About ESBG (European Savings and Retail Banking Group)

ESBG represents the locally focused European banking sector, helping savings and retail banks in 20 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 1,000 banks, which together employ 780,000 people driven to innovate at 56,000 outlets. ESBG members have total assets of €6.2 trillion, provide €500 billion in SME loans, and serve 150 million Europeans seeking retail banking services. ESBG members are committed to further unleash the promise of sustainable, responsible 21st century banking.

Learn more about ESBG at www.wsbi-esbg.org.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ▪ www.wsbi-esbg.org

Published by ESBG. [Date]