

**OPINION** 1 (6) Date 21 June 2022 Information classification Öppen Registration number A348.274/2022 Ref No 005

Swedish Police Authority

# **Opinion from the Swedish Police Authority concerning** the EDPB's Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement

The Swedish Police Authority recognises the need for EU-wide guidelines for the use of facial recognition technology in the area of law enforcement and therefore welcomes the fact that the European Data Protection Board has drawn up guidelines on this. This new technology is constantly evolving and there are various risks involved in its use that need to be addressed. In the view of the Swedish Police Authority, this technology can have a major positive impact in terms of both law enforcement and individuals' fundamental rights and freedoms. Clear guidelines can provide support in these important considerations. However, the Swedish Police Authority considers that the guidelines presented are unbalanced and will seriously impede and limit the development of effective and legally secure law enforcement methods. The Swedish Police Authority provides the following viewpoints.

# 2.1 One biometric technology, two distinct functions

The description of facial recognition technology (FRT) in this section lacks an essential element. The biometric templates that are produced can only be used in combination with the algorithm for which they were produced. In the description of storage in a database (point 9) and the subsequent descriptions of use, consideration must be given to the fact that the right algorithm needs to be available. The same applies to the risks associated with the unauthorised disclosure of face templates (see point 36 for example).

The algorithms used by the Swedish Police Authority will be handled in a very secure manner and will not be available for any use other than the legal and justified purposes that apply for the Swedish Police Authority. There is therefore no immediate risk that an unauthorised actor could garner personal information from a stored facial template.

## 3.1 General Legal Framework – The EU Charter of Fundamental Rights (hereinafter "the Charter") and the European Convention on Human Rights (ECHR)

## 3.1.1 Applicability of the Charter

The Swedish Police Authority agrees that the analysis of video footage collected in connection with the surveillance of an individual over time and in many different locations can provide information that maps out this individual's private and family life. However, the use of FRT to analyse such footage does not in itself provide access to any additional information than if the footage had been analysed manually. The primary purpose of using FRT is to reduce analysis time and improve the quality of analysis. In a preliminary investigation, FRT is typically used to analyse footage from a specific crime scene or close to a crime scene after an offence has been committed. In such cases, there is no surveillance of an individual over time and place that is intended to map out their life in the way described in the section (points 35 and 36). However, in some cases there may be a need for a law enforcement agency to map out where a certain individual has been within a wider area in order to investigate a serious offence. Software for image analysis may then contribute to privacy protection in that it minimises the detailed examination required by officers of the parts of the footage that are of direct interest for the purpose.

As described above in the comment on section 2.1, unauthorised access (point 36) to the biometric data that the facial templates represent poses less of a risk than access to a photograph does. For an unauthorised actor to be able to understand the facial template, they also need to have access to the algorithm for which the facial template was produced. For the same reason, a facial template cannot be easily used as a login method or cryptographic key for another system.

In light of this, the arguments outlined in the section concerning the risks of an impact on the right to a private and family life appear to be sweeping and unnuanced.

### 3.2 Specific legal framework – the Law Enforcement Directive

Concerning the permissibility of biometric data processing, the Swedish Police Authority would initially like to recall that the purpose of the Law Enforcement Directive<sup>1</sup> is also to enable a free flow of personal data within the EU that is not restricted for data protection reasons (Article 1(2)). In addition to the other provisions in the Law Enforcement Directive, the free flow of personal data must therefore not be restricted for data protection reasons.

The guidelines are based on the provisions of the EU Charter of Fundamental Rights concerning the conditions under which limitations may be permitted to the exercise of fundamental rights and freedoms (points 42–44 and points 69–70). The Swedish Police Authority would like to stress that there is already a legal basis in European Union law for such limitations as a result of biometric data processing through the regulations contained in the Law Enforcement Directive. In addition to the provisions in the Directive that regulate in particular the processing of biometric data, the provisions concerning the legal basis and the principles of all personal data processing set out the framework for biometric data processing and specify the conditions under which such processing is permitted. The Directive does not prohibit any specific use of biometric data. It should also be stressed that biometric data was not generally considered to be the kind of special category of personal data that required special regulations before the 2018 data protection reform.

Where the Swedish Police Authority is concerned, the Law Enforcement Directive has been implemented in Swedish law through a framework law, the Criminal Data Act (2018:1177), and a special law, the Act on Police personal data processing within the scope of the Criminal Data Act (2018:1693). In essence, the Swedish lawmakers have chosen not to separately regulate or specifically limit the possibilities for law enforcement agencies to use FRT, apart from having set the requirement that the biometric data processing must be absolutely necessary. It is also important that the legislation specifies at a fundamental level the objectives, what personal data is to be processed, the purpose of the processing, the procedures for protecting the privacy and confidentiality of personal data, and the procedures for its destruction so that there are sufficient guarantees against the risk of abuse or arbitrariness (ground 33 in the Law Enforcement Directive). Furthermore, it is the responsibility of each Swedish government agency to observe the proportionality requirement in all activities. Therefore, in the Swedish Police Authority's view, there must always be an overall assessment of all relevant provisions in national law when assessing the quality of the legislation as well as the foreseeability and the privacy protection offered by the law.

<sup>&</sup>lt;sup>1</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

21 June 2022 Reg No A348.274/2022 4 (6) Info class Öppen

For example, it is clear from the Swedish legislation and the preparatory work that Swedish law permits the use of FRT in law enforcement activities under the condition that it is strictly necessary, that the processing is carried out for specified, explicit and legitimate purposes, and that other relevant provisions are followed. This has also been the premise from which the Swedish Police Authority proceeded in its impact assessments prior to using FRT, which has been approved by the national supervisory authority during several prior consultations.

The technology is constantly evolving and it is difficult to predict what will be possible in the future. This applies not only to FRT. There is already a certain inertia in the legal processes, meaning that law enforcement agencies are not able to make full use of the technical possibilities despite the fact that this would be both legitimate and proportionate in a democratic society. The EDPB's proposed guidelines place very high demands for the national lawmakers in terms of regulating in detail and continuously following technological developments (cf. points 44 and 71-72). The Swedish Police Authority fears that these requirements, in combination with the already far reaching requirements laid out in data protection regulations in terms of protective measures, impact assessments and prior consultations with the supervisory authority, will result in limitations that are not proportionate to the justified needs of law enforcement agencies. The fact that legislation quickly becomes obsolete due to technological developments also risks having a negative impact on the protection of fundamental rights and freedoms. The Swedish Police Authority therefore considers that it is necessary to have flexible legislation that allows for balanced considerations on the basis of general principles, various kinds of risks and proportionality.

To avoid a situation in which there are different regulations and interpretations of European Union law, the Swedish Police Authority considers that the focus should primarily be on producing guidelines that provide guidance concerning the requirement *absolutely necessary* and the kind of technical and organizational protective measures that can guarantee the legal processing of personal data. This is also in line with the role that national data protection agencies have by offering prior consultations to provide advice and support to personal data controllers prior to processing that involves particular risks. It is difficult to see how requirements concerning the detailed national regulation of certain technology fit into this system.

### 3.2.1.2 Strictly Necessary

The Swedish Police Authority notes that the EDPB's interpretation of the requirement 'strictly necessary' means that the scope for law enforcement agencies to use FRT is limited to an absolute minimum. This in turn leads to a clear conflict with the efforts of the lawmakers and authorities to use the possibilities offered by technology to more effectively prevent and investigate crime and in doing so protect people's fundamental rights and freedoms. In the Swedish Police Authority's view, it should be taken into consideration that the alternative in certain cases to using software for image analysis to assist in search and analysis, for example, may instead involve a large number of officers going through huge quantities of images manually. Even if it is possible in theory (in some cases), this would mean needing to actually access a large number of irrelevant images and would require the images to be saved for a considerably longer period of time, which is difficult to reconcile with the general principles in data protection regulations.

#### 3.2.3 Categories of the data subjects

When searching through video footage during a preliminary investigation, it is necessary to be able to scan all faces that appear in the footage so as to identify the individual who is of interest to the investigation and map out the course of events. An approach in which FRT may not be used on individuals who fall outside the categories listed in Article 6 of the Law Enforcement Directive may result in a situation where it is not possible to use FRT in a fit-for-purpose manner in a preliminary investigation.

#### **Consequences for law enforcement**

Overall, the Swedish Police Authority considers that the requirements for detailed regulations described in the guidelines would lead to major challenges for law enforcement agencies in their efforts to carry out their assignment using modern technology. It would also be impossible in practice for national lawmakers to draw up and keep up to date the kind of legislation that the EDPB appears to advocate. The guidelines limit the use of FRT to an "absolute minimum", which in the Swedish Police Authority's view is clearly stricter than what for instance was stated by the Swedish lawmakers when the Directive was implemented. It is also difficult to foresee what impact the guidelines will have on the assessment of the processing of biometric data other than facial templates. In several respects the guidelines are sweeping and unnuanced. In addition to the points made above, the Swedish Police Authority would like to stress the importance of distinguishing between situations in which the technology is used for profiling/automated decisions and when it merely helps officers to find the right information in a large amount of material, for example, and to make their own correct assessments. The Swedish Police Authority would also like to point out that no competent authority has claimed that FRT or any other new technology is a "silver bullet" (point 102) and can replace traditional methods. However, modern technology can be an important and natural aid that contributes both to legally secure and effective law enforcement and to protecting people's fundamental rights and freedoms.

#### Conclusion

The Swedish Police Authority recognises the need for guidelines for the use of FRT within law enforcement and therefore welcomes the fact that the EDPB has drawn up these guidelines. However, the Swedish Police Authority considers that the proposed guidelines will seriously impede and limit law enforcement agencies' possibilities of processing biometric data in general and using FRT in particular, in a way that is not compatible with the purposes of the Law Enforcement Directive. The EDPB should consider this and the other viewpoints provided by the Swedish Police Authority in the final design of the guidelines.

This opinion has been decided by National Police Commissioner Anders Thornberg. Reporting clerk was Legal Adviser Abir Tasci.

#### THE SWEDISH POLICE AUTHORITY

Anders Thornberg

bir Jasi

Abir Tasci