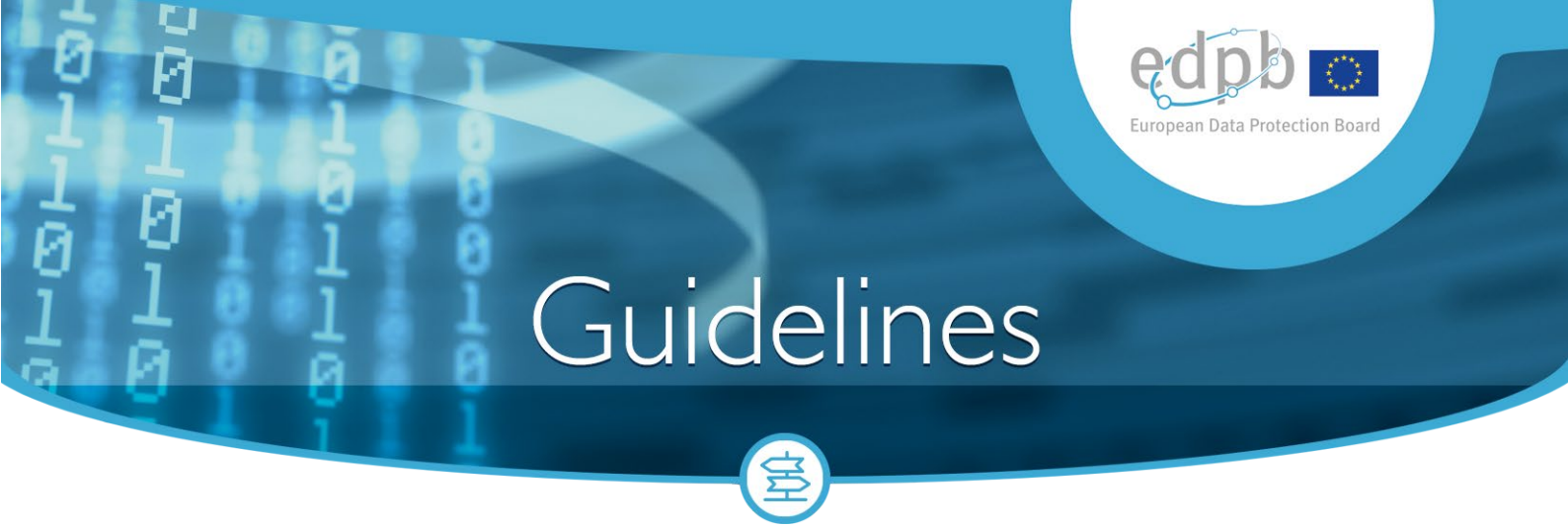

Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement

Version 2.0

Adopted on 26 April 2023

Version history

Version 1.0	12 May 2022	Adoption of the Guidelines for public consultation
Version 2.0	26 April 2023	Adoption of the Guidelines after public consultation

Table of content

EXECUTIVE SUMMARY

More and more law enforcement authorities (LEAs) apply or intend to apply facial recognition technology (FRT). It may be used to **authenticate** or to **identify** a person and can be applied on videos (e.g. CCTV) or photographs. It may be used for various purposes, including to search for persons in police watch lists or to monitor a person's movements in the public space.

FRT is built on the processing of **biometric data**, therefore, it encompasses the processing of special categories of personal data. Often, FRT uses components of **artificial intelligence** (AI) or machine learning (ML). While this enables large scale data processing, it also induces the risk of discrimination and false results. FRT may be used in controlled 1:1 situations, but also on huge crowds and important transport hubs.

FRT is a **sensitive tool for LEAs.** LEAs are executive authorities and have sovereign powers. FRT is prone to interfere with fundamental rights – also beyond the right to protection of personal data – and is able to affect our social and democratic political stability.

For personal data protection in the law enforcement context, the **requirements of the LED** have to be met. A certain framework regarding the use of FRT is provided for in the LED, in particular Article 3(13) LED (term "biometric data"), Article 4 (principles relating to processing of personal data), Article 8 (lawfulness of processing), Article 10 (processing of special categories of personal data) and Article 11 LED (automated individual decision-making).

Several other fundamental rights may be affected by the application of FRT as well. Hence, the **EU Charter of Fundamental Rights** ("the Charter") is essential for the interpretation of the LED, in particular the right to protection of personal data of Article 8 of the Charter, but also the right to privacy laid down in Article 7 of the Charter.

Legislative measures that serve as a legal basis for the processing of personal data directly interfere with the rights guaranteed by Articles 7 and 8 of the Charter. The processing of biometric data under all circumstances constitutes a serious interference in itself. This does not depend on the outcome, e.g. a positive matching. Any limitation to the exercise of fundamental rights and freedoms must be provided for by law and respect the essence of those rights and freedoms.

The legal basis must be **sufficiently clear** in its terms to give citizens an adequate indication of conditions and circumstances in which authorities are empowered to resort to any measures of collection of data and secret surveillance. A mere transposition into domestic law of the general clause in Article 10 LED would lack precision and foreseeability.

Before the national legislator creates a new legal basis for any form of processing of biometric data using facial recognition, the competent data protection supervisory authority should be **consulted**.

Legislative measures have to be **appropriate** for attaining the legitimate objectives pursued by the legislation at issue. An **objective of general interest** – however fundamental it may be – does not, in itself, justify a limitation to a fundamental right. Legislative measures should **differentiate** and target those persons covered by it in the light of the objective, e.g. fighting specific serious crime. If the measure covers all persons in a general manner without such differentiation, limitation or exception, it intensifies the interference. It also intensifies the interference if the data processing covers a significant part of the population.

The data has to be processed in a way that ensures the applicability and effectiveness of the EU data protection rules and principles. Based on each situation, the **assessment of necessity and proportionality** has to also identify and consider all possible implications for other fundamental rights. If the data is systematically processed without the knowledge of the data subjects, it is likely to generate a **general feeling of constant surveillance**. This may lead to chilling effects in regard of some or all of the fundamental rights concerned, such as human dignity under Article 1 of the Charter, freedom of thought, conscience and religion under Article 10 of the Charter, freedom of expression under Article 11 of the Charter as well as freedom of assembly and association under Article 12 of the Charter.

Processing of special categories of data, such as biometric data can only be regarded as "**strictly necessary**" (Art. 10 LED) if the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary, i.e. indispensable, and excluding any processing of a general or systematic nature.

The fact that a photograph has been **manifestly made public** (Art. 10 LED) by the data subject does not entail that the related biometric data, which can be retrieved from the photograph by specific technical means, is considered as having been manifestly made public. Default settings of a service, e.g. making templates publicly available, or absence of choice, e.g. templates are made public without the user being able to change this setting, should not in any way be construed as data manifestly made public.

Article 11 LED establishes a framework for **automated individual decision-making**. The use of FRT entails the use of special categories of data and may lead to profiling, depending on the way and purpose FRT is applied for. In any case, in accordance with Union law and Article 11(3) LED, profiling that results in discrimination against natural persons on the basis of special categories of personal data shall be prohibited.

Article 6 LED regards the necessity to **distinguish between different categories of data subjects**. With regard to data subjects for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with the legitimate aim according to the LED, there is most likely no justification of an interference.

The **data minimisation principle** (Art. 4(1)(e) LED) also requires that any video material not relevant to the purpose of the processing should always be removed or anonymised (e.g. by blurring with no retroactive ability to recover the data) before deployment.

The controller must carefully consider how to (or if it can) meet the requirements for **data subject's rights** before any FRT processing is launched since FRT often involves processing of special categories of personal data without any apparent interaction with the data subject.

The effective exercise of data subject's rights is dependent on the controller fulfilling its **information obligations** (Art. 13 LED). When assessing whether a "specific case" according to Article 13(2) LED exists, several factors need to be taken into consideration, including if personal data is collected without the knowledge of the data subject as this would be the only way to enable data subjects to effectively exercise their rights. Should decision-making be done solely based on FRT, then the data subjects need to be informed about the features of the automated decision making.

As regards **access requests**, when biometric data is stored and connected to an identity also by alpha-numerical data, in line with the principle of data minimization, this should allow for the competent authority to give confirmation to an access request based on a search by those alpha-numerical data

and without launching any further processing of biometric data of others (i.e. by searching with FRT in a database).

The risks for the data subjects are particularly serious if inaccurate data is stored in a police database and/or shared with other entities. The controller must **correct** stored data and FRT systems accordingly (see also recital 47 LED).

The right to **restriction** becomes especially important when it comes to facial recognition technology (based on algorithm(s) and thereby never showing a definitive result) in situations where large quantities of data are gathered and the accuracy and quality of the identification may vary.

A **data protection impact assessment (DPIA)** before the use of FRT is a mandatory requirement, cf. Article 27 LED. The EDPB recommends making public the results of such assessments, or at least the main findings and conclusions of the DPIA, as a trust and transparency enhancing measure.

Most cases of deployment and use of FRT contain intrinsic high risk to the rights and freedoms of data subjects. Therefore, the authority deploying the FRT should **consult** the competent supervisory authority prior to the deployment of the system.

Given the unique nature of biometric data, the authority, implementing and/or using FRT should pay special attention to the **security of processing**, in line with Article 29 LED. In particular, the law enforcement authority should ensure that the system complies with the relevant standards and implements biometric template protection measures. Data protection principles and safeguards must be embedded in the technology before the start of the processing of personal data. Therefore, even when a LEA intends to apply and use FRT from external providers, it has to ensure, e.g. through the procurement procedure, that only FRT built upon the principles of **data protection by design and by default** are deployed.

Logging (cf. Art. 25 LED) is an important safeguard for verification of the lawfulness of the processing, both internally (i.e. self-monitoring by the concerned controller/processor) and by external supervisory authorities. In the context of facial recognition systems, logging is recommended also for changes of the reference database and for identification or verification attempts including user, outcome and confidence score. Logging, however, is just one essential element of the overall **principle of accountability** (cf. Art. 4(4) LED). The controller has to be able to demonstrate the compliance of the processing with the basic data protection principles of Article 4(1)-(3) LED.

The EDPB recalls its and the EDPS' joint **call for a ban** of certain kinds of processing in relation to (1) remote biometric identification of individuals in publicly accessible spaces, (2) AI-supported facial recognition systems categorising individuals based on their biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation or other grounds for discrimination (3) use of facial recognition or similar technologies, to infer emotions of a natural person and (4) processing of personal data in a law enforcement context that would rely on a database populated by collection of personal data on a mass-scale and in an indiscriminate way, e.g. by "scraping" photographs and facial pictures accessible online.

A central safeguard to the fundamental rights at stake is **effective supervision** by the competent data protection supervisory authorities. Therefore, Member States have to ensure that the resources of the supervisory authorities are appropriate and sufficient to allow them to fulfil their mandate.

These **guidelines address** law makers at EU and national level, as well as LEAs and their officers implementing and using FRT-systems. Individuals are addressed as far as they are interested generally or as data subjects, in particular as regards data subjects' rights.

The **guidelines intend** to inform about certain properties of FRT and the applicable legal framework in the context of law enforcement (in particular the LED).

- In addition, they provide a **tool to support a first classification of the sensitivity of a given use case** (Annex I).
- They also contain **practical guidance for LEAs that wish to procure and run a FRT-system** (Annex II).
- The guidelines also depict several typical **use cases and list numerous considerations relevant**, especially with regard to the necessity and proportionality test (Annex III).

1 INTRODUCTION

1. Facial recognition technology (FRT) may be used to automatically recognise individuals based on their face. FRT often is based on artificial intelligence such as machine learning technologies. Applications of FRT are increasingly tested and used in various areas, from individual use to private organisations and public administration use. Law enforcement authorities (LEAs) also expect advantages from the use of FRT. It promises solutions to relatively new challenges such as investigations involving a big amount of captured evidence, but also to known problems, in particular with regard to under-staffing for observation and search tasks.

2. A great deal of the increased interest in FRT is based on the efficiency and scalability of FRT. With these come the disadvantages inherent to the technology and its application – also on a large scale. While there may be thousands of personal data sets analysed at the push of a button, already slight effects of algorithmic discrimination or misidentification may create high numbers of individuals affected severely in their conduct and daily lives. The sheer size of processing of personal data, and in particular biometric data, is a further key element of FRT, as the processing of personal data constitutes an interference with the fundamental right to protection of personal data according to Article 8 of the Charter of Fundamental Rights of the European Union (the Charter).

3. The application of FRT of LEAs will – and to some extent already does – have significant implications on individuals and on groups of people, including minorities. These implications will also have considerable effects on the way we live together and on our social and democratic political stability, valuing the high significance of pluralism and political opposition. The right to protection of personal data often is key as a prerequisite to guarantee other fundamental rights. The application of FRT is considerably prone to interfere with fundamental rights beyond the right to protection of personal data.

4. The EDPB therefore deems it important to contribute to the ongoing integration of FRT in the area of law enforcement covered by the Law Enforcement Directive[1] respectively the national laws transposing it and provide the present guidelines. The guidelines are intended to provide relevant information to lawmakers at EU and national level, as well as for LEAs and their officers when implementing and using FRT-systems. The scope of the guidelines is limited to FRT. However, other forms of processing of personal data based on biometrics by LEAs, especially if processed remotely, may entail similar or additional risks for individuals, groups and society. According to the respective

[1] 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.

circumstances, some aspects of these guidelines may serve as a useful source in these cases, as well. Finally, individuals that are interested generally or as data subjects may also find important information, in particular as regards data subjects' rights.

5. The guidelines consist of the main document and three annexes. The main document at hand presents the technology and the legal framework applicable. To help identifying some of the major aspects to classify the severity of the interference with fundamental rights to a given field of application, a template can be found in Annex I. LEAs that wish to procure and run a FRT system may find practical guidance in Annex II. Depending on the field of application of FRT, different considerations could be of relevance. A set of hypothetical scenarios and relevant considerations may be found in Annex III.

2 TECHNOLOGY

2.1 One biometric technology, two distinct functions

6. Facial recognition is a probabilistic technology that can automatically recognise individuals based on their face in order to authenticate or identify them.

7. FRT falls into the broader category of biometric technology. Biometrics include all automated processes used to recognise an individual by quantifying physical, physiological or behavioural characteristics (fingerprints, iris structure, voice, gait, blood vessel patterns, etc.). These characteristics are defined as "biometric data", because they allow or confirm the unique identification of that person.

8. This is the case with people's faces or, more specifically, their technical processing using facial recognition devices: by taking the image of a face (a photograph or video) called a biometric "sample", it is possible to extract a digital representation of distinct characteristics of this face (this is called a "template").

9. A biometric template is a digital representation of the unique features that have been extracted from a biometric sample and can be stored in a biometric database[2]. This template is supposed to be unique and specific to each person and it is, in principle, permanent over time[3]. In the recognition phase, the device compares this template with other templates previously produced or calculated directly from biometric samples such as faces found on an image, photo or video. "Facial recognition" is therefore a two-step process: the collection of the facial image and its transformation into a template, followed by the recognition of this face by comparing the corresponding template with one or more other templates.

10. Like any biometric process, facial recognition can fulfil two distinct functions:

- the **authentication** of a person, aimed at verifying that a person is who she or he claims to be. In this case, the system will compare a pre-recorded biometric template or sample (e.g. stored on a smartcard or biometric passport) with a single face, such as that of a person turning up at a checkpoint, in order to verify whether this is one and the same person. This functionality therefore relies on the comparison of two templates. This is also called 1-to-1 **verification**.

- the **identification** of a person, aimed at finding a person among a group of individuals, within a specific area, an image or a database. In this case, the system must process each face captured, to generate a biometric template and then check whether it matches with a person known to the

[2] Guidelines on facial recognition, Consultative Committee of Convention 108 the Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, June 2021.
[3] This might depend on the type of biometry and the age of the data subject.

system. This functionality thus relies on comparing one template with a database of templates or samples (baseline). This is also called 1-to-many identification. For example, it can link a personal name record (surname, first name) to a face, if the comparison is made against a database of photographs associated with surnames and first names. It can also involve following a person through a crowd, without necessarily making the link with the person's civil identity.

11. In both cases, the used facial recognition techniques are based on an estimated match between templates: the one being compared and the baseline(s). From this point of view, they are probabilistic: the comparison deduces a higher or lower probability that the person is indeed the person to be authenticated or identified; if this probability exceeds a certain threshold in the system, defined by the user or the developer of the system, the system will assume that there is a match.

12. While both functions – authentication and identification – are distinct, they both relate to the processing of biometric data related to an identified or identifiable natural person and therefore constitute a processing of personal data, and more specifically a processing of special categories of personal data.

13. Facial recognition is part of a wider spectrum of video image processing techniques. Some video cameras can film people within a defined area, in particular their faces, but they cannot be used as such to automatically recognise individuals. The same applies to simple photography: a camera is not a facial recognition system because photographs of people need to be processed in a specific way in order to extract biometric data.

14. The mere detection of faces by so-called "smart" cameras does not necessarily constitute a facial recognition system either. While they also raise important questions in terms of ethics and effectiveness, digital techniques for detecting abnormal behaviours or violent events, or for recognising facial emotions or even silhouettes, they may not be considered as biometric systems processing special categories of personal data, provided that they do not aim at uniquely identifying a person and that the personal data processing involved does not include other special categories of personal data. These examples are not completely unrelated to facial recognition and are still subject to personal data protection rules.[4] Furthermore, this type of detection system may be used in conjunction with other systems aiming at identifying a person and thereby being considered as a facial recognition technology.

15. Unlike video capture and processing systems, for example, which require the installation of physical devices, facial recognition is a software functionality which can be implemented within existing systems (cameras, image databases, etc.). Such functionality can therefore be connected or interfaced with a multitude of systems, and combined with other functionalities. Such integration into an already existing infrastructure requires specific attention because it comes with inherent risks due to the fact that the facial recognition technology could be frictionless and easily hidden[5].

2.2 A wide variety of purposes and applications

16. Beyond the scope of these guidelines and outside the scope of the LED, facial recognition may be used for a wide variety of objectives, both for commercial use and for addressing public safety or law enforcement concerns. It may be applied in many different contexts: in the personal relationship between a user and a service (access to an application), for access to a specific place (physical filtering),

[4] Article 10 LED (or Article 9 GDPR) is applicable, however, to systems that are used to categorise individuals based on their biometrics into clusters according to ethnicity as well as political or sexual orientation or other special categories of personal data.

[5] For instance, in body-worn cameras which are increasingly being used in practice.

or without any particular limitation in the public space (live facial recognition). It can be applied to any kind of data subject: a customer of a service, an employee, a simple onlooker, a wanted person or someone implicated in legal or administrative proceedings, etc. Some uses are already commonplace and widespread; others are, at this point, at the experimental or speculative stage. While these guidelines will not be addressing all such uses and applications, the EDPB recalls that they may only be implemented if compliant with the applicable legal framework, and in particular with the GDPR and relevant national laws.[6] Even in the context of the LED, further to the functions of authentication or identification, data processed with the use of facial recognition technology can also be further processed for other purposes, such as categorisation.

17. More specifically, a scale of potential uses might be considered depending on the degree of control people have over their personal data, the effective means they have for exercising such control and their right to initiative to trigger and use of this technology, the consequences for them (in the case of recognition or non-recognition) and the scale of the processing carried out. Facial recognition based on a template stored on a personal device (smartcard, smartphone, etc.) belonging to that person, used for authentication and of strictly personal use through a dedicated interface, does not pose the same risks as, for example, usage for identification purposes, in an uncontrolled environment, without the active involvement of the data subjects, where the template of each face entering the monitoring area is compared with templates from a broad cross-section of the population stored in a database. Between these two extremes lies a very varied spectrum of uses and associated issues related to the protection of personal data.

18. In order to further illustrate the context within which facial recognition technologies are currently being debated or implemented, either for authentication or identification, the EDPB deems relevant to mention a series of examples. The examples below are solely descriptive and should not be considered as any kind of preliminary assessment of their compliance with the EU acquis in the field of data protection.

Examples of facial recognition authentication

19. Authentication can be designed for users to have full control over it, for example to enable access to services or applications purely within a home setting. As such, it is used extensively by smartphone owners to unlock their device, instead of password authentication.

20. Facial recognition authentication may also be used to check the identity of someone hoping to benefit from public or private third-party services. Such processes thus offer a way of creating a digital identity using a mobile app (smartphone, tablet, etc.) which can then be used to access online administrative services.

21. Furthermore, facial recognition authentication can aim at controlling physical access to one or more predetermined locations, such as entrances to buildings or specific crossing points. This functionality is, for example, implemented in certain processing for the purpose of border crossing, where the face of the person at the checkpoint device is compared with the one stored in their identity document (passport or secure residence permit).

Examples of facial recognition identification

[6] See also EDPB guidelines 3/2019 on processing of personal data through video devices adopted on 29 January 2020, for further guidance.

22. Identification may be applied in many, even more diverse ways. These particularly include, but are not limited to, the uses listed below, currently observed, experimented or planned in the EU.

- searching, in a database of photographs, for the identity of an unidentified person (victim, suspect, etc.);
- monitoring of a person's movements in the public space. His or her face is compared with the biometric templates of people travelling or having travelled in the monitored area, for example when a piece of luggage is left behind or after a crime has been committed;
- reconstructing a person's journey and their subsequent interactions with other persons, through a delayed comparison of the same elements in a bid to identify their contacts for example;
- remote biometric identification of wanted persons in public spaces. All faces captured live by video-protection cameras are cross-checked, in real time, against a database held by the security forces;
- automatic recognition of people in an image to identify, for example, their relationships on a social network, which uses it. The image is compared with the templates of everyone on the network who has consented to this functionality in order to suggest the nominative identification of these relationships;
- access to services, with some cash dispensers recognising their customers, by comparing a face captured by a camera with the database of facial images held by the bank;
- tracking of a passenger's journey at a certain stage of the journey. The template, calculated in real time, of any person checking in at gates located at certain stages of the journey (baggage drop-off points, boarding gates, etc.), is compared with the templates of people previously registered in the system.

23. In addition to the use of FRT in the field of law enforcement, the wide range of applications observed certainly calls for a comprehensive debate and policy approach in order to ensure consistency and compliance with the EU acquis in the field of data protection.

2.3 Reliability, accuracy and risks for data subjects

24. Like every technology, facial recognition may also be subject to challenges when it comes to its implementation, in particular when it comes to its reliability and efficiency in terms of authentication or identification, as well as the overall issue of quality and accuracy of the "source" data and the result of facial recognition technology processing.

25. Such technological challenges entail particular risks for data subjects concerned which are all the more significant or serious in the area of law enforcement considering the possible effects for data subjects either legal, or other ones similarly affecting them in a significant manner. In this context, it appears also useful to underline that the ex post use of FRT is not per se safer, as individuals may be tracked across time and places. Thus, the ex post use also poses specific risks which have to be assessed on a case-by-case basis. [7]

26. As pointed out by the EU Fundamental Rights Agency in its 2019 report, "determining the necessary level of accuracy of facial recognition software is challenging: there are many different ways to evaluate and assess accuracy, also depending on the task, purpose and context of its use. When

[7] See the examples presented in Annex III.

applying the technology in places visited by millions of people – such as train stations or airports – a relatively small proportion of errors (e.g. 0.01%)[8] still means that hundreds of people are wrongly flagged. In addition, certain categories of people may be more likely to be wrongly matched than others, as described in Section 3. There are different ways to calculate and interpret error rates, so caution is required. In addition, when it comes to accuracy and errors, questions in relation to how easily a system can be tricked by, for example, fake face images (called 'spoofing') are important particularly for law enforcement purposes."[9]

27. In this context, the EDPB considers it important to recall that FRT, whether used for the purposes of authentication or identification, do not provide for a definitive result but rely on probabilities that two faces, or images of faces, correspond to the same person.[10] This result is further degraded when the quality of biometric sample input to the facial recognition is low. Blurriness of input images, low resolution of camera, motion and low light, can be factors of low quality. Other aspects with significant impact on the results are prevalence and spoofing, e.g. when criminals try to either avoid passing by the cameras or to trick the FRT. Numerous studies have also highlighted that such statistical results from algorithmic processing may also be subject to bias, notably resulting from the source data quality as well as training databases, or other factors, like the choice of location of the deployment. Furthermore, one should also highlight the impact of facial recognition technology on other fundamental rights, such as the respect for private and family life, freedom of expression and information, freedom of assembly and association, etc.

28. It is therefore essential that the reliability and accuracy of facial recognition technology is taken into account as criteria for the assessment of compliance with key data protection principles, as per Article 4 LED, and in particular when it comes to fairness and accuracy.

29. While highlighting that high-quality data is essential for high quality algorithms, the EDPB also stresses the need for data controllers, as part of their accountability obligation, to undertake regular and systematic evaluation of algorithmic processing in order to ensure in particular the accuracy, fairness and reliability of the result of such personal data processing. Personal data used for the purposes of evaluating, training and further developing FRT systems may only be processed on the basis of a sufficient legal basis and in accordance with the common data protection principles.

3 APPLICABLE LEGAL FRAMEWORK

30. The use of facial recognition technologies is intrinsically linked to processing of personal data, including special categories of data. Moreover, it has direct or indirect impact on a number of fundamental rights, enshrined in the EU Charter of Fundamental Rights. This is particularly relevant in the area of law enforcement and criminal justice. Therefore, any use of facial recognition technologies should be carried out in strict compliance with the applicable legal framework.

31. The following information is intended to be used for consideration when assessing future legislative and administrative measures as well as implementing existing legislation on a case-by-case basis that involves FRT. The relevance of the respective requirements varies according to the particular

[8] This accuracy rate stems from the report quoted and reflects a rate much better than the current performance of algorithms in applications of FRT.
[9] Facial recognition technology: fundamental rights considerations in the context of law enforcement, EU Fundamental Right Agency, 21st November 2019.
[10] This probability is referred to as "confidence score".

circumstances. As not all future circumstances may be foreseen, it is only considered to be providing support and not to be interpreted as an exhaustive enumeration.

3.1 General legal framework – The EU Charter of Fundamental Rights and the European Convention on Human Rights (ECHR)

3.1.1 Applicability of the Charter

32. The EU Charter of Fundamental Rights (hereinafter "the Charter") is addressed to the institutions, bodies, offices and agencies of the Union and to the Member States when they are implementing Union law.

33. Regulating the processing of biometric data for law enforcement purposes according to Article 1(1) LED inevitably raises the question of compliance with fundamental rights, in particular the respect for private life and communications under Article 7 of the Charter and the right to protection of personal data under Article 8 of the Charter.

34. The collection and analysis of video footage of natural persons, including their faces, implies the processing of personal data. When technically processing the image, the processing also covers biometric data. The technical processing of data relating to the face of a natural person in relation to time and place allows conclusions to be drawn concerning the private lives of the relevant persons. Those conclusions may refer to the racial or ethnic origins, health, religion, habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. The great range of the information that may be revealed by the application of FRT clearly shows the possible impact on the right to the protection of personal data laid down in Article 8 of the Charter, but also on the right to privacy laid down in Article 7 of the Charter.

35. In such circumstances it is also not inconceivable that the collection, analysis and further processing of the biometric (facial) data in question might have an effect on the way that people feel free to act even if the act would be fully within the remits of a free and open society. It might also have severe implications on the exercise of their fundamental rights, such as their right to freedom of thought, conscience and religion, expression of peaceful assembly and freedom of association under Articles 1, 10, 11 and 12 of the Charter. Such processing also involves other risks, such as the risk of abuse of the personal information gathered by the relevant authorities as a result of unlawful access to and use of the personal data, security breach etc. The risks often depend on the processing and its circumstances, such as the risk of unlawful access and use by police officers or by other unauthorised parties. However, some risks simply are inherent to the unique nature of biometric data. Unlike an address or a telephone number, it is impossible for a data subject to change his or her unique characteristics, such as the face or the iris. In the case of unauthorised access or accidental publication of biometric data, this would lead to the data being compromised in their use as passwords or cryptographic keys or could be used for further, unauthorised surveillance activities to the detriment of the data subject.

3.1.2 Interference with the rights laid down in the Charter

36. The processing of biometric data under all circumstances constitutes a serious interference in itself. This does not depend on the outcome, e.g. a positive matching. The processing constitutes an interference even if the biometric template is immediately deleted after the matching against a police database results in a no-hit.

37. The interference with the fundamental rights of the data subjects may stem from an act of law that either aims at or has the effect of restricting the respective fundamental right[11]. It may also result from an act of a public authority with the same purpose or effect or even of a private entity entrusted by law to exercise public authority and public powers.

38. A legislative measure that serves as a legal basis for the processing of personal data directly interferes with the rights guaranteed by Articles 7 and 8 of the Charter[12].

39. The use of biometric data and FRT in particular in many cases also affects the right to human dignity, guaranteed by Article 1 of the Charter. Human dignity requires that individuals are not treated as mere objects. FRT calculates existential and highly personal characteristics, the facial features, into a machine-readable form with the purpose of using it as a human license plate or ID card, thereby objectifying the face.

40. Such a processing may also interfere with other fundamental rights, such as the rights under Articles 10, 11 and 12 of the Charter insofar as chilling effects are either intended by or derive from the relevant video surveillance of law enforcement agencies.

41. In addition, the potential risks generated by the use of facial recognition technologies by law enforcement with regard to the right to fair trial and the presumption of innocence under Articles 47 and 48 of the Charter should also be carefully considered. The outcome of the application of FRT, e.g. a match, may not only lead to a person being subject to further policing, but also be decisive evidence in court proceedings. Shortcomings of FRT such as possible bias, discrimination or wrong identification ('false positive') may thus lead to severe implications also on criminal proceedings. Furthermore, in the assessment of evidence, the outcome of the application of FRT may be favoured, even if there is contradicting evidence ('automation bias').

3.1.3 Justification for the interference

42. According to Article 52(1) of the Charter, any limitation to the exercise of fundamental rights and freedoms must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

3.1.3.1 Provided for by law

43. Article 52(1) of the Charter sets the requirement of a specific legal basis. This legal basis must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which authorities are empowered to resort to any measures of collection of data and secret surveillance[13]. It must indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities so as to ensure individuals the minimum degree of protection as entitled under the rule of law in a democratic society[14]. Moreover, lawfulness requires adequate safeguards to ensure that in particular an individual's right under Article 8 of the Charter is respected. These principles also apply to the processing of personal data for purposes of evaluating, training and further developing of FRT systems.

[11] CJEU, C-219/91 – Ter Voort, RoC 1992 I-05485, para. 36f.; CJEU, C-200/96 – Metronome, RoC 1998 I-1953, para. 28.
[12] CJEU, C-594/12, para. 36; CJEU, C-291/12, para. 23 and the following.
[13] ECtHR, Shimovolos v. Russia, § 68; Vukota-Bojić v. Switzerland.
[14] ECtHR, Piechowicz v. Poland, § 212.

44. Given that biometric data when processed for the purpose of uniquely identifying a natural person constitute special categories of data listed in Article 10 LED, the different applications of FRT in most cases would require a dedicated law precisely describing the application and the conditions for its use. This encompasses in particular the types of crime and, where applicable, the appropriate threshold of severity of these crimes, in order to, among other things, effectively exclude petty crime.[15]

3.1.3.2 The essence of the fundamental right to privacy and to protection of personal data laid down in Articles 7 and 8 of the Charter

45. The limitations of the fundamental rights imminent to each situation still have to provide for the essence of the particular right to be respected. The essence refers to the very core of the relevant fundamental right[16]. Human dignity has to be respected too, even where a right is restricted[17].

46. Indications of a possible infringement of the inviolable core are the following:

- A provision that imposes limitations irrespective of a person's individual conduct or exceptional circumstances[18].
- The recourse to the courts is not possible or hindered[19].
- Prior to a severe limitation, the circumstances of the individual concerned are not taken into account[20].
- With a view to the rights under Articles 7 and 8 of the Charter: In addition to a broad collection of communication meta-data, the acquisition of the knowledge of the content of the electronic communication could violate the essence of those rights[21].
- With a view to the rights under Articles 7, 8 and 11 of the Charter: Legislation which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, inter alia, personal data relating to those services[22].
- With reference to the rights under Article 8 of the Charter: A lack of basic principles of data protection and data security could also infringe the core of the right[23].

3.1.3.3 Legitimate aim

47. As already explained in point 3.1.3., limitations to the fundamental rights have to genuinely meet objectives of general interest recognised by the European Union or meet the need to protect the rights and freedoms of others.

48. Recognised by the Union are both the objectives mentioned in Article 3 of the Treaty on the European Union and other interests protected by specific provisions of the Treaties[24], i.e. – inter alia – an area of freedom, security and justice, the prevention and combating of crime. In its relations with the wider world, the Union should contribute to peace and security and the protection of human rights.

---

[15] See e.g. CJEU judgments in cases C-817/19 Ligue des droits humains, para. 151 f, C-207/16 Ministerio Fiscal, para. 56.
[16] CJEU C-279/09, RoC 2010 I-13849, para. 60.
[17] Explanations relating to the Charter of Fundamental Rights, Title I, Explanation on Article 1, OJ C 303, 14.12.2007, p. 17–35.
[18] CJEU C-601/15, para 52.
[19] CJEU C-400/10, RoC 2010 I-08965, para. 55.
[20] CJEU C-408/03, RoC 2006 I-02647, para. 68.
[21] CJEU - 203/15 - Tele2 Sverige, para. 101 with reference to CJEU - C-293/12 and C-594/12, para. 39.
[22] CJEU C-512/18, La Quadrature du Net, para. 209 et seq.
[23] CJEU - C-594/12, para. 40.
[24] Explanations relating to the Charter of Fundamental Rights, Title I, Explanation on Article 52, OJ C 303, 14.12.2007, p. 17–35.

49. The need to protect the rights and freedoms of others refers to rights of persons that are protected by the law of the European Union or of its Member States. The assessment must be carried out with the aim to reconcile the requirements of the protection of the respective rights and to strike a fair balance between them[25].

3.1.3.4 Necessity and proportionality test

50. Where interferences with fundamental rights are at issue, the extent of the national and Union legislator's discretion may prove to be limited. This depends on a number of factors, including the area concerned, the nature of the right in question guaranteed by the Charter, the nature and seriousness of the interference and the objective pursued by the interference[26]. Legislative measures have to be appropriate for attaining the legitimate objectives pursued by the legislation at issue. Moreover, the measure must not exceed the limits of what is appropriate and necessary in order to achieve those objectives[27]. An objective of general interest – however fundamental it may be – does not, in itself, justify a limitation to a fundamental right[28].

51. According to the CJEU's settled case-law, derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary[29]. This also implies that there are no less intrusive means available to achieve the purpose. Possible alternatives such as – depending on the given purpose – additional staffing, more frequent policing or additional street lighting have to be carefully identified and assessed. Legislative measures should differentiate and target those persons covered by it in the light of the objective, e.g. fighting serious crime. If it covers all persons in a general manner without such differentiation, limitation or exception, it intensifies the interference[30]. It also intensifies the interference if the data processing covers a significant part of the population[31].

52. The protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter[32]. Legislation must lay down clear and precise rules governing the scope and application of the measure in question and impose safeguards so that the persons whose data have been processed have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access or use of that data[33]. The need for such safeguards is all the greater where personal data is subject to automatic processing and where there is a significant risk of unlawful access to the

---

[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31-32.
[26] CJEU - C-594/12, para. 47 with the following sources: see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V.
[27] CJEU - C-594/12, para. 46 with the following sources: Case C-343/09 Afton Chemical EU:C:2010:419, paragraph 45; Volker und Markus Schecke and Eifert EU:C:2010:662, paragraph 74; Cases C-581/10 and C-629/10 Nelson and Others EU:C:2012:657, paragraph 71; Case C-283/11 Sky Österreich EU:C:2013:28, paragraph 50; and Case C- 101/12 Schaible EU:C:2013:661, paragraph 29.
[28] CJEU - C-594/12, para. 51.
[29] CJEU - C-594/12, para. 52, with the following sources: Case C-473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited.
[30] CJEU - C-594/12, para. 57.
[31] CJEU - C-594/12, para. 56.
[32] CJEU - C-594/12, para. 53.
[33] CJEU - C-594/12, para. 54, with the following sources: see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, § 62 and 63; Rotaru v. Romania, § 57 to 59, and S. and Marper v. the United Kingdom, § 99.

data[34]. Furthermore, internal or external, e.g. judicial, authorisation of the deployment of FRT may also contribute as safeguards, and may prove to be necessary in certain cases of severe interference.[35]

53. The rules laid down have to be adapted to the specific situation, e.g. the quantity of data processed, the nature of the data[36] and the risk of unlawful access to the data. This calls for rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality[37].

54. With regard to the relationship between the controller and the processor it should not be permitted for the processors to have regard only to economic considerations when determining the level of security which they apply to personal data; this could endanger a sufficient high level of protection[38].

55. An act of law has to lay down substantive and procedural conditions and objective criteria by which to determine the limits of competent authorities' access to data and their subsequent use. For the purposes of prevention, detection or criminal prosecutions, the offences concerned would have to be considered sufficiently serious to justify the extent and seriousness of these interferences with the fundamental rights enshrined for example in Articles 7 and 8 of the Charter[39].

56. The data has to be processed in a way that ensures the applicability and effect of the EU data protection rules; in particular those provided by Article 8 of the Charter, which states that the compliance with the requirements of protection and security shall be subject to control by an independent authority. The geographical place where the processing takes place may in such a situation be relevant[40].

57. With regard to the different steps of processing of personal data, a distinction should be made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned[41]. The determination of the conditions of the processing, for example, the determination of the retention period, must be based on objective criteria in order to ensure that the interference is limited to what is strictly necessary[42].

58. Based on each situation, the assessment of necessity and proportionality has to identify and consider all implications that fall within the scope of other fundamental rights, such as human dignity under Article 1 of the Charter, freedom of thought, conscience and religion under Article 10 of the Charter, freedom of expression under Article 11 of the Charter as well as freedom of assembly and association under Article 12 of the Charter.

59. Furthermore, it has to be considered as a matter of severity, that if the data is systematically processed without the knowledge of the data subjects, it is likely to generate a general conception of constant

[34] CJEU - C-594/12, para. 55, with the following sources: see, by analogy, as regards Article 8 of the ECHR, S. and Marper v. the United Kingdom, § 103, and M. K. v. France, 18 April 2013, no. 19522/09, § 35.
[35] ECtHR, Szabó and Vissy v. Hungary, §§ 73-77.
[36] See also the heightened requirements for technical and organizational measures when processing special categories of data, Article 29 para. 1 LED.
[37] CJEU - C-594/12, para. 66.
[38] CJEU - C-594/12, para. 67.
[39] CJEU - C-594/12, para. 60 and 61.
[40] CJEU - C-594/12, para. 68.
[41] CJEU - C-594/12, para. 63.
[42] CJEU - C-594/12, para. 64.

surveillance[43]. This may lead to chilling effects in regard of some or all of the fundamental rights concerned.

60. In order to facilitate and operationalise the assessment of necessity and proportionality in legislative measures related to facial recognition in the law enforcement area, the national and Union legislators could take advantage of the available practical tools especially designed for this task. In particular, the necessity and proportionality toolkit[44] provided by the European Data Protection Supervisor could be used.

3.1.3.5 Articles 52(3), 53 of the Charter (level of protection, also in relation to that of the ECHR)

61. According to Article 52(3) and Article 53 of the Charter, the meaning and scope of those rights of the Charter that correspond to the rights guaranteed in the ECHR must be the same as those laid down by the ECHR. While in particular for Article 7 of the Charter an equivalent may be found in the ECHR, this is not the case for Article 8 of the Charter[45]. Article 52(3) of the Charter does not prevent Union law to provide more extensive protection. As the ECHR does not constitute a legal instrument which has been formally incorporated into EU law, EU legislation must be undertaken in the light of the fundamental rights of the Charter[46].

62. According to Article 8 of the ECHR, there shall be no interference by a public authority with the exercise of this right to respect for private and family life except when in accordance with the law and what is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

63. The ECHR also sets standards with regard to the way limitations can be undertaken. One basic requirement, besides the rule of law, is foreseeability. In order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures[47]. This requirement is acknowledged by the CJEU and EU data protection law (cf. section 3.2.1.1).

64. Further specifying the rights of Article 8 ECHR, the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[48] have to be fully respected too. Still, it has to be considered that these provisions represent only a minimum standard in view of the prevailing Union law.

3.2 Specific legal framework – the Law Enforcement Directive

[43] CJEU - C-594/12, para. 37.
[44] European Data Protection Supervisor: Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit (11.4.2017); European Data Protection Supervisor: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019).
[45] CJEU - C-203/15 - Tele2 Sverige, para 129.
[46] CJEU – C-311/18, para. 99.
[47] European Court of Human Rights, Judgment, CASE OF COPLAND v. THE UNITED KINGDOM, 03/04/2007, Application no. 62617/00, para 46.
[48] ETS No. 108.

65. A certain framework regarding the use of FRT is provided for in the LED. First of all, Article 3(13) LED defines the term "biometric data"[49]. For details, cf. section 2.1 above. Secondly, Article 8(2) clarifies that in order for any processing to be lawful it must – besides being necessary for the purposes stated in Article 1(1) LED – be regulated in national law that specifies at least the objectives of the processing, the personal data to be processed and the purpose of the processing. Further provisions of special relevance with regard to biometric data are Articles 10 and 11 LED. Article 10 has to be read in connection with Article 8 LED[50]. The principles for processing personal data as laid down in Article 4 LED should always be adhered to and any assessment of possible biometric processing via FRT should be guided by these.

3.2.1 Processing of special categories of data for law enforcement purposes

66. According to Article 10 LED, processing of special categories of data, such as biometric data, shall be allowed only where strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject. In addition thereto, it shall only be allowed, where authorised by Union or Member State law, to protect the vital interests of the data subject or of another natural person, or where such processing relates to data which is manifestly made public by the data subject. This general clause highlights the sensitivity of the processing of special categories of data.

3.2.1.1 Authorised by Union or Member State Law

67. Regarding the necessary type of legislative measure, recital 33 LED states that "[w]here this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned."[51].

68. According to Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter shall be 'provided for by law'. This echoes the expression 'in accordance with the law' in Article 8(2) of the ECHR, which means not only compliance with applicable law, but also relates to the quality of that law without prejudice to the nature of the act, requiring it to be compatible with the rule of law.

69. Recital 33 LED states further that "[h]owever, such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction".

70. The national law must be sufficiently clear in its terms to give data subjects an adequate indication of the circumstances in and conditions under which controllers are empowered to resort to any such measures. This includes possible preconditions for processing like specific types of evidence as well as the necessity of judicial or internal authorisation. The respective law may be technology neutral as far as the specific risks and characteristics of the processing of personal data by FRT systems are sufficiently addressed. In line with the LED and the case law of the Court of Justice of the European

[49] Art. 3(13) LED: 'Biometric data' means 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.
[50] WP258, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), p. 7.
[51] The type of legislative measures considered has to be in line with EU law or with the national law. Depending on the degree of interference of the restriction, a particular legislative measure, taking into account the level of norm, could be required at national level.

Union (CJEU) and of the European Court of Human Rights (ECtHR), it is indeed essential that legislative measures, which aim to provide a legal basis for a facial recognition measure, are foreseeable for the data subjects.

71. A legislative measure cannot be invoked as a law authorising the processing of biometric data by means of FRT for law enforcement purposes if it is a mere transposition of the general clause in Article 10 LED.

72. Apart from biometric data, Article 10 LED regulates the processing of other special categories of data such as sexual orientation, political opinions and religious beliefs, thus covering a broad range of processing. In addition, such a provision would lack specific requirements indicating the circumstances in and conditions under which law enforcement authorities would be empowered to resort to using facial recognition technology. Due to the reference to other types of data and the explicit need for special safeguards without further specifications, the national provision transposing Article 10 LED into national law - with a similarly general and abstract wording - cannot be invoked as a legal basis for the processing of biometric data involving facial recognition, as it would lack precision and foreseeability. In line with Articles 28(2) or 46(1)(c) LED, before the legislator creates a new legal basis for any form of processing of biometric data using facial recognition, the national data protection supervisory authority should be consulted.

3.2.1.2 Strictly Necessary

73. Processing can only be regarded as "strictly necessary" if the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary[52]. The addition of the term "strictly" means that the legislator intended the processing of special categories of data to only take place under conditions even stricter than the conditions for necessity (see above, item 3.1.3.4). This requirement should be interpreted as being indispensable. It restricts the margin of appreciation permitted to the law enforcement authority in the necessity test to an absolute minimum. In accordance with the settled case-law of the CJEU, the condition of "strict necessity" is also closely linked to the requirement of objective criteria in order to define the circumstances and conditions under which processing can be undertaken, thus excluding any processing of a general or systematic nature[53].

3.2.1.3 Manifestly Made Public

74. When assessing whether processing relates to data which are manifestly made public by a data subject, it should be recalled that a photograph as such is not systematically considered to be biometric data[54]. Therefore, the fact that a photograph has been manifestly made public by the data subject does not entail that the related biometric data, which can be retrieved from the photograph by specific technical means, is considered as having been manifestly made public.

75. As for personal data in general, for biometric data to be seen as manifestly made public by the data subject, the data subject must have deliberately made the biometric template (and not simply a facial image) freely accessible and public through an open source. If a third party discloses the biometric data, it cannot be considered that the data has been manifestly made public by the data subject.

---

[52] Consistent case law on the fundamental right to respect for private life, see CJEU Case C-73/07 para. 56 (Satakunnan Markkinapörssi and Satamedia); CJEU, Cases C-92/09 and C-93/09 para. 77 (Schecke and Eifert); CJEU - C-594/12, para. 52 (Digital Rights); CJEU Case C-362/14 para. 92 (Schrems).

[53] CJEU Case C-623/17, para 78.

[54] Cf. recital 51 of the GDPR: « the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. »

76. Moreover, it is not sufficient to interpret the behaviour of a data subject to consider that biometric data has been manifestly made public. For example, in the case of social networks or online platforms, the EDPB considers that the fact that the data subject did not trigger or set specific privacy features is not sufficient to consider that this data subject has manifestly made public its personal data and that this data (e.g. photographs) can be processed into biometric templates and used for identification purposes without the data subject's consent. More generally, default settings of a service, e.g. making templates publicly available, or absence of choice, e.g. the templates are made public without the user to be able to change this setting, should not in any way be construed as data manifestly made public.

3.2.2 Automated individual decision-making, including profiling

77. Article 11(1) LED provides for the duty of the Member States to generally prohibit decisions based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her. As an exemption to this general prohibition, such processing may be possible only if authorised by Union or Member State law to which the controller is subject to and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller. It may only be used restrictively. This threshold applies for ordinary (i.e. not special) categories of personal data. An even higher threshold and more restrictive usage applies for the exemption under Article 11(2) LED. It re-emphasises that decisions under the first paragraph shall not be based on special categories of data, i.e. in particular biometric data for the purpose of uniquely identifying a natural person. An exemption may only be foreseen if suitable measures to safeguard the data subject's rights and freedoms and legitimate interests of the natural person concerned are in place. This exemption must be read in addition to and in the light of the premises of Article 10 LED.

78. Depending on the FRT system, even human intervention assessing the results of FRT may not necessarily provide for a sufficient guarantee by itself in respecting individuals' rights and in particular the right to the protection of personal data, considering the possible bias and error that can result from the processing itself. Furthermore, human intervention may only be considered as a safeguard if the person intervening may critically challenge the results of FRT during human intervention. It is crucial to enable the person to understand the FRT system and its limits as well as to interpret its results properly. It is also necessary to establish a work place and organisation that counteracts the effects of automation bias, and avoids fostering the uncritical acceptance of the results e.g. by time pressure, burdensome procedures, potential detrimental career effects etc.

79. According to Article 11(3) LED, profiling that results in discrimination against natural persons on the basis of special categories of personal data such as biometric data shall be prohibited, in accordance with Union law. According to Article 3(4) LED, 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. When considering whether suitable measures to safeguard the data subject's rights and freedoms and legitimate interests of the natural person concerned are foreseen, it has to be kept in mind that the use of FRT may lead to profiling, depending on the way and purpose that the FRT is applied for. In any case, in accordance with Union law and Article 11(3) LED, profiling that results in discrimination against natural persons on the basis of special categories of personal data shall be prohibited.

3.2.3 Categories of the data subjects

80. Article 6 LED regards the necessity to distinguish between different categories of data subjects. This distinction has to be made where applicable and as far as possible. It has to show effect in the way the data are processed. From the examples given in Article 6 LED it can be inferred that, as a rule, the processing of personal data has to meet the criteria of necessity and proportionality also with regard to the category of data subjects[55]. It can further be inferred that with regard to data subjects for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with the legitimate aim according to the LED, there is most likely no justification of an interference[56]. If no distinction according to Article 6 LED is applicable or possible, the exception from the rule of Article 6 LED has to be rigorously considered in the assessment of the necessity and proportionality of the interference. The distinction between different categories of data subjects appears as an essential requirement when it comes to personal data processing involving facial recognition, also considering the possible false positive or false negative hits, which can have significant impacts for data subjects as well as in the course of an investigation.

81. As said, when implementing Union law, the provisions of the Charter of Fundamental Rights of the European Union have to be respected, cf. Article 52 of the Charter. The framework and criteria that the LED provides are therefore to be read in the light of the Charter. Acts of law of the EU and its Member States must not fall below this measure and have to ensure the Charter's full effect.

3.2.4 Rights of the data subject

82. The EDPB has already provided guidance on data subjects' rights under the GDPR in different aspects[57]. The LED provides for similar data subject rights and general guidance on this has been provided in an opinion by Article 29 WP, which has been endorsed by the EDPB[58]. Under certain circumstances, the LED allows for some limitations to these rights. The parameters for such limitations will be further elaborated in section 3.2.4.6. "Legitimate limitations to data subject's rights".

83. While all data subject's rights as listed in Chapter III of the LED, naturally apply also to personal data processing via facial recognition technology (FRT), the following chapter will focus on some of the rights and aspects that might be of particular interest to receive guidance on. Furthermore, this chapter and its analysis is incumbent on the FRT processing in question having passed through the legal requirements as described in the previous chapter.

84. Given the nature of personal data processing through FRT (processing of special categories of personal data often without any apparent interaction with the data subject) the controller must carefully consider how to (or if it can) meet the requirements of the LED before any FRT processing is launched. In particular by carefully analysing:

- who the data subjects are (often more than the one(s) that is the main target for the purpose of processing),
- how the data subjects are made aware of the FRT processing (see section 3.2.4.1),

[55] Cf. also CJEU - C-594/12, para. 56 – 59.
[56] Cf. also CJEU - C-594/12, para. 58.
[57] See for example 1/2022 EDPB Guidelines on data subject's rights – Right of access and 3/2019 EDPB Guidelines on processing of personal data through video devices.
[58] WP258, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680).

- how the data subjects can exercise their rights (here both information and access rights as well as rights to rectification or restriction can be particularly challenging to uphold in case FRT is used for all but 1-to-1 verification in direct contact with the data subject).

3.2.4.1 Making rights and information known to data subjects in a concise, intelligible and easily accessible form

85. FRT provides for challenges in ensuring that data subjects are made aware of their biometric data being processed. It is particularly challenging if a LEA is analysing through FRT video material that derives from or is provided by a third party since there is little possibility, and most of the time none, for the LEA to notify the data subject at the time of collection (e.g. via a sign on-site). Any video material not relevant to the investigation (or purpose for processing) should always be removed or anonymised (e.g. by blurring with no retroactive ability to recover the data) before deploying any processing of biometric data, in order to avoid the risk of not having fulfilled the minimisation principle in Article 4(1)(e) LED and the information obligations in Article 13(2) LED. It is the responsibility of the controller to assess what information would be of importance for the data subject in exercising his or her rights and to ensure that the necessary information is provided. The effective exercise of data subject's rights is dependent on the controller fulfilling its information obligations.

86. Article 13(1) LED stipulates what minimum information needs to be provided to the data subject in general. This information may be provided for via the controller's website, in printed form (e.g. a leaflet available on demand), or otherwise easy-to-access sources for the data subject. The data controller must in any event ensure that information is effectively provided in relation to at least the following elements:

- identity and contact details of the controller, including the Data Protection Officer,
- the purpose of the processing and that it is processing via FRT,
- the right to lodge a complaint with a supervisory authority and contact details of such authority,
- the right to request access to, and rectification or erasure of, personal data and restriction of processing of the personal data.

87. In addition, in specific cases as defined in national law which should be in line with Article 13(2) LED[59], as for example FRT processing, the following information needs to be provided directly to the data subject:

- the legal basis for the processing,
- information on where the personal data was collected without the data subject's knowledge,
- the period for which the personal data will be stored, or where that is not possible, the criteria used to determine that period,
- if applicable, the categories of recipients of the personal data (including third countries or international organisations).

88. While Article 13(1) LED is about general information made available to the public, Article 13(2) LED is about the additional information to be provided to a particular data subject in specific cases, for example where data is collected directly from the data subject or indirectly without the knowledge of

[59] E.g. Section 56 (1) of the German Federal Data Protection Act which, amongst other, states what information needs to be provided to data subjects in undercover operations

the data subject[60]. There is no clear definition of what is meant with "specific cases" in Article 13(2) LED. However, it refers to situations where the data subjects need to be made aware of the processing that refers to them specifically and be provided with appropriate information in order to effectively exercise their rights. The EDPB considers that when assessing whether a "specific case" exists, several factors need to be taken into consideration, including if personal data is collected without the knowledge of the data subject, as this would be the only way to enable data subjects to effectively exercise their rights. Other examples of "specific cases" could be where personal data is further processed as subject to an international criminal cooperation procedure or in the situation of personal data being processed under covert operations as specified in national law. Furthermore, it follows from recital 38 LED that should decision-making be done solely based on FRT, then the data subjects need to be informed about the features of the automated decision making. This would also indicate that this is a specific case where additional information should be provided to the data subject in accordance with Article 13(2) LED[61].

89. Finally, it should be noted that according to Article 13(3) LED, Member States may adopt legislative measures that restrict the obligation to provide information in specific cases for certain objectives. This applies to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the data subject.

3.2.4.2 Right to access

90. In general, the data subject has the right to receive positive or negative confirmation of any processing of his or her personal data and, where the answer is positive, the access to the personal data as such, plus additional information, as listed in Article 14 LED. For FRT, when biometric data is stored and connected to an identity also by alpha-numerical data, this should allow for the competent authority to give confirmation to an access request based on a search by those alpha-numerical data and without launching any further processing of biometric data of others (i.e. by searching with FRT in a database). The principle of data minimisation must be observed and no more data than is necessary with regard to the purpose of the processing should be stored.

3.2.4.3 Right to rectification of personal data

91. Since FRT does not provide for absolute accuracy, it is of particular importance that controllers are vigilant to requests for rectification of personal data. It may also be the case when a data subject based on FRT has been placed in an inaccurate category, e.g. wrongfully put in the category of suspects based on initial assumption of course of action in a video footage. The risks for the data subjects are particularly serious if such inaccurate data is stored in a police database and/or shared with other entities. The controller must correct stored data and FRT systems accordingly, see recital 47 LED.

3.2.4.4 Right to erasure

92. FRT will under most circumstances – in case not used for 1-to-1 verification/authentication – amount to the processing of a large number of data subjects' biometric data. It is therefore important that the controller beforehand considers where the limits to its purpose and necessity lies, so that a request for erasure in accordance with Article 16 LED can be dealt with without undue delay (since the controller needs, among others, to erase personal data that is processed beyond what the applicable legislation following Articles 4, 8 and 10 LED allows for).

---

[60] WP258 Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), p.17-18

[61] Note well the difference between "made available to the data subject" in Article 13(1) LED and "give to the data subject" in Article 13(2) LED. In Article 13(2) LED the controller must ensure that the information reaches the data subject, where published information on a website will not be sufficient.

3.2.4.5 Right to restriction

93. In case the accuracy of the data is contested by the data subject and the accuracy of the data cannot be ascertained (or when the personal data must be maintained for the purpose of future evidence), the controller has an obligation to restrict personal data of that data subject in accordance with Article 16 LED. This becomes especially important when it comes to facial recognition technology (based on algorithm(s) and thereby never showing a definitive result) in situations where large quantities of data are gathered and the accuracy and quality of the identification may vary. With poor quality video material (e.g. from a crime scene) the risk of false positives increases. Furthermore, if facial images in a watch list are not regularly updated that will also increase the risk of false positives or false negatives. In specific cases, where data cannot be erased due to the fact that there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject, the data should instead be restricted and processed only for the purpose which prevented their erasure (see recital 47 LED).

3.2.4.6 Legitimate limitations to data subject's rights

94. When it comes to the information obligations of the controller and the data subjects´ right of access, limitations are allowed only so long as they are laid down in the law which in turn needs to constitute a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned (see Articles 13(3), 13(4) 15 and 16(4) LED). When FRT is used for law enforcement purposes one can expect it to be used under circumstances where it would be harmful for the purpose pursued to inform the data subject or to allow access to the data. This would apply for instance to a police investigation of a crime or in order to protect national security or public security.

95. The right of access does not automatically mean access to all the information e.g. in a criminal case where one's personal data occurs. A viable example of when limitations to the right may be allowed could be during the course of a criminal investigation.

3.2.4.7 Exercise of rights through the supervisory authority

96. In cases where there are legitimate limitations to the exercise of rights according to Chapter III LED, the data subject may request the data protection authority to exercise his or her rights on their behalf by checking the lawfulness of the controller's processing. It falls on the controller to inform the data subject of the possibility of exercising their rights in such way (see Article 17 LED and Article 46(1)(g) LED). For FRT it means that the controller has to ensure that appropriate measures are in place so that such a request can be handled, e.g. enabling the search of recorded material provided that the data subject provides sufficient information in order to locate the personal data of him or her.

3.2.5 Other legal requirements and safeguards

3.2.5.1 Article 27 Data protection impact assessment

97. A data protection impact assessment (DPIA) before the use of FRT is a mandatory requirement since the type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons. Given that the use of FRT entails systematic automatic processing of special categories of data, it could it be assumed that in such cases the controller would be, as a rule, required to conduct a DPIA. The DPIA should contain as a minimum a general description of the envisaged processing operations, an assessment of the necessity and proportionality of the processing operations in relation to the purposes, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance. The EDPB recommends making public the

results of such assessments, or at least the main findings and conclusions of the DPIA, as a trust and transparency enhancing measure[62].

3.2.5.2 Article 28 Prior consultation of the supervisory authority

98. Pursuant to Article 28 LED, the controller or processor has to consult the supervisory authority prior to the processing, where: (a) a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or (b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects. As already explained in section 2.3. of these guidelines, the EDPB considers that most cases of deployment and use of FRT contain intrinsic high risk to the rights and freedoms of data subjects. Therefore, in addition to the DPIA, the authority deploying the FRT should consult the competent supervisory authority, prior to the deployment of the system.

3.2.5.3 Article 29 Security of processing

99. The unique nature of biometric data makes it impossible for a data subject to change it, in case it is compromised, e.g. as a result of a data breach. Therefore, the competent authority, implementing and/or using FRT should pay special attention to the security of processing, in line with Article 29 LED. In particular, the law enforcement authority should ensure the system complies with the relevant standards and implement biometric template protection measures[63]. This obligation is even more relevant if the law enforcement authority is using a third-party service provider (data processor).

3.2.5.4 Article 20 Data protection by design and by default

100. Data protection by design and by default, in accordance with Article 20 LED, is aimed at ensuring that the data protection principles and safeguards, such as data minimisation and storage limitation, are embedded in the technology through appropriate technical and organisational measures, such as pseudonymisation, even before the start of the processing of personal data and will be applied throughout its lifecycle. Given the inherent high risk for the rights and freedoms of natural persons, the choice of such measures should not depend solely on economic considerations[64] but should instead strive to implement the state-of-art in data protection technologies. In the same vein, if a LEA intends to apply and use FRT from external providers, it has to ensure, for instance through the procurement procedure, that only FRT built upon the principles of data protection by design and by default are deployed[65]. This also implies that transparency on the functioning of FRT is not limited by claims of trade secrets or intellectual property rights.

3.2.5.5 Article 25 Logging

101. The LED stipulates different methods of demonstrating by the controller or the processor the lawfulness of the processing and ensuring data integrity and data security. In this regard, system logs are a very useful tool and an important safeguard for verification of the lawfulness of the processing, both internally (i.e. self-monitoring) and by external supervisory authorities, such as the data protection authorities. Pursuant to Article 25 LED, logs for at least the following processing operations should be kept in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. Moreover, the logs of consultation and disclosure

[62] For more information see WP248 rev.01 Data protection impact assessment Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk".

[63] See for example: ISO/IEC 24745 Information security, cybersecurity and privacy protection — Biometric information protection.

[64] See recital 53 of the LED.

[65] For more information see EDPB Guidelines on Data Protection by Design and by Default, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

should make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data. Furthermore, in the context of facial recognition systems, logging of the following additional processing operations is recommended (partly beyond Article 25 LED):

- Changes of the reference database (addition, deletion or update). The log should keep a copy of the relevant (added, deleted or updated) image, when it is not otherwise possible to verify the lawfulness or the outcome of the processing operations.
- Identification or verification attempts including the outcome and confidence score. Strict minimisation principle should apply, so that only the identifier of the image from the reference database is kept in the logs, instead of storing the reference image. Logging the input biometric data should be avoided unless there is necessity (e.g. only in match cases)
- The ID of the user who requested the identification or verification attempt.
- Any personal data stored in the logs of the systems are subject to strict purpose limitations (e.g. audits) and should not be used for other purposes (e.g. to be able to still perform recognition/verification including an image that has been deleted from the reference databases). Security measures should be applied to ensure the integrity of the logs, whereas automatic monitoring systems to detect abuse of logs are highly recommended. For the reference database logs, security measures should be equivalent to the reference database, in case of facial images storage. Also, automatic processes to ensure the enforcement of the data retention period for the logs should be implemented.

3.2.5.6 Article 4(4) Accountability

102. The controller has to be able to demonstrate the compliance of the processing with the principles of Article 4 (1)-(3), cf. Article 4(4) LED. A systematic and up-to-date documentation of the system (including updates, upgrades and algorithmic training), the technical and organisational measures (including system performance monitoring and potential human intervention) and the processing of the personal data is crucial in this regard. To demonstrate the lawfulness of the processing, a particularly important element is logging according to Article 25 LED (cf. section 3.2.5.5). The accountability principle not only refers to the system and the processing, but also to the documentation of procedural safeguards such as necessity and proportionality assessments, DPIAs as well as internal consultations (e.g. management approval of the project or internal decisions on confidence score values) and external consultations (e.g. DPA). Annex II includes a number of elements in this regard.

3.2.5.7 Article 47 Effective supervision

103. The effective supervision by the competent data protection authorities is one of the most important safeguards for the fundamental rights and freedoms of the individuals affected by the use of FRT. At the same time, providing each data protection authority with the necessary human, technical and financial resources, premises and infrastructure is a prerequisite for the effective performance of their tasks and exercise of their powers[66]. Even more crucial than the number of available staff, are the skills of the experts, who should cover a very broad range of issues - from criminal investigations and police cooperation to big data analytics and AI. Therefore, Member States should ensure that the resources

[66] See Commission Communication "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", COM(2022) 364 final, p. 3.4.1.

of the supervisory authorities are appropriate and sufficient to allow them to fulfil their mandate to protect the rights of data subjects and closely follow any developments in this regard.[67]

4 CONCLUSION

104. The use of facial recognition technologies is intrinsically linked to processing of significant amounts of personal data, including special categories of data. The face and, more generally, biometric data are permanently and irrevocably linked to a person's identity. Therefore, the use of facial recognition has direct or indirect impact on a number of fundamental rights and freedoms enshrined in the EU Charter of Fundamental Rights that may go beyond privacy and data protection, such as human dignity, freedom of movement, freedom of assembly, and others. This is particularly relevant in the area of law enforcement and criminal justice.

105. The EDPB understands the need for law enforcement authorities to benefit from the best possible tools to quickly identify the perpetrators of terrorist acts and other serious crimes. However, such tools should be used in strict compliance with the applicable legal framework and only in cases when they satisfy the requirements of necessity and proportionality, as laid down in Article 52(1) of the Charter. Moreover, while modern technologies may be part of the solution, they are by no means a 'silver bullet'.

106. There are certain use cases of facial recognition technologies, which pose unacceptably high risks to individuals and society ('red lines'). For these reasons the EDPB and the EDPS have called for their general ban[68].

107. In particular, remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into individuals' private lives and does not have a place in a democratic society, as by its nature, it entails mass surveillance. In the same vein, the EDPB considers AI-supported facial recognition systems categorising individuals based on their biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation as not compatible with the Charter. Furthermore, the EDPB is convinced that the use of facial recognition or similar technologies, to infer emotions of a natural person is highly undesirable and should be prohibited, possibly with few duly justified exceptions. In addition, the EDPB considers that processing of personal data in a law enforcement context that would rely on a database populated by collection of personal data on a mass-scale and in an indiscriminate way, e.g. by "scraping" photographs and facial pictures accessible online, in particular those made available via social networks, would, as such, not meet the strict necessity requirement provided for by Union law.

5 ANNEXES

Annex I: Support Pattern

Annex II: Practical guidance for managing FRT projects in LEAs

[67] See Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, para. 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

[68] See EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

Annex III: Practical Examples

ANNEX I - TEMPLATE FOR DESCRIPTION OF SCENARIOS

(With infoboxes for aspects dealt within the scenario)

Description of the processing:

- Description of the processing, Context (crime relation), Purpose

Source of information:

- Types of data subjects: ☐ all citizens ☐ convicts ☐ suspects
  ☐ children ☐ other vulnerable data subjects
- Source of image: ☐ publicly accessible spaces ☐ internet
  ☐ private entity ☐ other individuals ☐ other …….
- Connection to crime: ☐ Direct temporal ☐ Not direct temporal
  ☐ Direct geographical ☐ Not direct geographical
  ☐ Not necessary
- Mode of information capture: ☐ remote ☐ in a booth or controlled environment
- Context- affecting other fundamental rights:
  ☐ No
  Yes, namely ☐ freedom of assembly
  ☐ Freedom of speech
  ☐ various:……
- Possibilities for additional sources of information about the data subject:
  ☐ ID document ☐ public telephone use ☐ vehicle license plate
  ☐ other …….

Reference database (to which captured information is compared):

- Specificity: ☐ general purpose databases ☐ specific databases related to crime area
- Description of how these reference databases were populated (and legal basis)
- Change of purpose of database (e.g. security of private property was the primary goal):☐ YES
  ☐ NO

Algorithm:

- Processing type: ☐ 1-1 verification (authentication) ☐ 1-many identification
- Accuracy considerations
- Technical safeguards

Outcome:

- Impact ☐ Direct (e.g. the data subject may be arrested, questioned, discriminatory behavior)
  ☐ Not direct (used for statistical models, no serious legal action against data subjects)
- Automated decision: ☐ YES ☐ NO
- Duration of storage

Legal analysis:

- Necessity and proportionality analysis - purpose/seriousness of crime/number of persons not involved but affected by processing
- Type of prior information to data subject: ☐ When entering the specific area
  ☐ In the LEA's website in general
  ☐ In the LEA's website for the specific processing
  ☐ Other .....
- Applicable legal framework:
  ☐ LED mostly copied to national law
  ☐ Generic national law for the use of biometric data by LEAs
  ☐ Specific national law for this processing (facial recognition) for that competent authority
  ☐ Specific national law for this processing (automated decision)

Conclusion:

General considerations as to whether the described processing is likely compatible with EU Law (and some hints to legal prerequisites)

ANNEX II- PRACTICAL GUIDANCE FOR MANAGING FRT PROJECTS IN LEAS

This Annex provides some additional practical guidance for Law Enforcement Authorities ("LEAs") planning to initiate a project involving Facial Recognition Technology ("FRT"). It provides more information on organizational and technical measures to consider during the deployment of the project and should not be considered as an exhaustive list of steps/measures to take. It should also be seen in conjunction with the EDPB Guidelines 3/2019 on processing of personal data through video devices[69] and any EU/EEA regulation and EDPB guidelines regarding the use of Artificial Intelligence.

This Annex provides guidelines based on the assumption that LEAs will procure FRT (as off-the-shelf products). If the LEA plans to develop (further train) the FRT, then additional requirements apply for selecting the necessary training, validation and testing datasets to be used during development and the roles/measures for the development environment. Similarly, an off-the-shelf product may require further adjustments for the intended use, in which case above mentioned requirements for the selection of testing, validation and training datasets should be met.

Belonging to the same LEA does not provide on its own full access to biometric data. As with any other personal data categories, biometric data collected for a certain law enforcement purpose under a specific legal basis cannot be used without a proper legal basis for a different law enforcement purpose (Article 4(2) of Directive (EU) 2016/680 (LED)). Also, developing/training an FRT tool is considered a different purpose and it should be assessed whether processing biometric data to measure performance/train the technology so to avoid impact on the data subjects by low performance is necessary and proportionate taking into account the initial purpose of processing.

1. ROLES AND RESPONSIBILITIES

When a LEA employs FRTs for the performance of its tasks falling under the scope of the LED (prevention, investigation detection or prosecution of criminal offences, etc., according to Article 3 LED), it can be considered the controller for the FRT. However, LEAs are composed of several units/departments that may be involved in this processing, either by defining the process of FRT application, or by applying it in practice. Due to the specificities of this technology, different units may need to be involved to either support in the measurements of its performance, or to further train it.

In a project involving FRT, there are several stakeholders[70] within LEAs that may need to be involved:

- Top management - to approve the project after balancing the risks against the potential benefits.
- DPO and/or legal department of the LEA - to assist in assessing the lawfulness of implementing a certain FRT project; to assist in carrying out the DPIA; to ensure the respect and exercise of the rights of the data subjects.

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[70] The following roles are indicative of the different stakeholders and their responsibilities in an FRT project. While the language used to describe the roles in this annex is not assertive, each LEA needs to define and assign similar roles according to its organisation. It might be the case that a unit accumulates more than one role, for instance process owner and reference database manager, or process owner and IT AI and/or Data Science Department (in case the unit of the process owner has all necessary technical knowledge).

- Process Owner - acting as the specific unit within the competent LEA to develop the project, deciding the details of the FRT project, including the system performance requirements; deciding on the appropriate fairness metric; setting the confidence score[71]; setting acceptable thresholds for bias; identifying the potential risks the FRT project poses for the rights and freedoms of the individuals (by consulting also the DPO and the IT AI and/or Data Science Department (see below) and to present them to the top management. The process owner will also consult the reference database manager, before deciding on the details of the FRT project, to understand both the use purpose of the reference database but also its technical details. In case of re-training a procured FRT, the Process Owner will also be in charge of the selection of the training dataset. As being the unit tasked with developing and deciding the details of the project, the process Owner is in charge of conducting the DPIA.
- IT AI and/or Data Science Department - to assist in carrying out a DPIA; to explain the metrics available to measure the system performance, fairness[72] and potential bias; to implement the technology and the technical safeguards, in order to prevent unauthorized access to the collected data, cyberattacks, etc. In case of re-training a procured FRT, the IT AI or Data science department will train the system, based on the training dataset provided by the Process Owner. This department will also be in charge of setting up the measures to mitigate the risks jointly identified by the process owners (e.g. AI specific risks such as model inference attacks).
- End users (such as the police officers in the field or in forensics labs) - to carry out a comparison against the database; to critically review the results taking into account previous evidence and provide feedback to the Process Owner for false positive results and indications of possible discrimination.
- Reference database manager - the specific unit within the competent LEA in charge of accumulating and managing the reference database, meaning the database against which images will be compared, including deleting facial images after the defined retention period. Such database can be created specifically for the envisaged FRT project or can pre-exist, for compatible purposes. The reference database manager is in charge of defining when and under which circumstances facial images can be stored as well as setting their data retention requirements (according to time or other criteria).

As most cases of deployment and use of FRT contain intrinsic high risk to the rights and freedoms of data subjects, the Data Protection Supervisory Authority should also be involved in the context of the prior consultation required by Article 28 LED.

2. INCEPTION/BEFORE PROCURING THE FRT SYSTEM

The Process Owner in a LEA should first have a clear understanding of the process(es) pursuing the use of FRT (the use case/s) and ensure there is a legal basis to ground the intended use case. Based on this, they need to:

- Describe formally the use case. The problem to be solved and the way FRT will provide a solution is to be described, as well as the overview of the process (task) in which it will be applied. In this regard, the LEAs should document at least[73]:

[71] Confidence score is the confidence level of the prediction (match), in the form of a probability. E.g. by comparing two templates, there is 90% confidence that these belong to the same person. Confidence score is different than the performance of the FRT, however it affects the performance. The higher the confidence threshold, the fewer false positives and more false negatives in the results of FRT.

[72] Fairness can be defined as the lack of unfair, unlawful discrimination, such as gender or race bias.

[73] Annex I provides a list of elements assisting the controller to describe an FRT use case.

- The categories of personal data recorded in the process
- The objectives and concrete purposes for which the FRT will be used, including the potential consequences for the data subject after a match.
- When and how the facial images will be collected (including information on the context of this collection, e.g. at the airport gate, videos from security cameras outside a store where a crime was committed etc. and the categories of data subjects whose biometric data will be processed).
- The database against which images will be compared (reference database), as well as information on how it was created, its size and the quality of biometric data it contains.
- The LEA actors who will be authorized to use the FRT system and act upon it in the law enforcement context (their profiles and access rights have to be defined by the Process Owner).
- The envisaged retention period for the input data, or the moment that will determine the end of this period (such as the closure or termination of the criminal proceedings in accordance with national procedural law for which they have been initially collected), as well as any subsequent action (deletion of this data, anonymisation and use for statistical or research purposes etc.).
- Logging implementation and accessibility of logs and records kept.
- The performance metrics (e.g. accuracy, precision, recall, F1-score) and their minimum acceptable thresholds.[74]
- An estimation of how many people will be subject to FRT in which time period / occasion.

- Perform a necessity and proportionality assessment[75]. The fact that this technology exists should not be the driver to apply it. The Process Owner must first assess whether an appropriate legal basis for the envisaged processing exists. For this, the DPO and the legal service need to be consulted. The driver to deploy FRT should be that it is necessary and proportionate solution for a specifically defined problem of LEAs. This needs to be assessed according to the purpose/seriousness of crime/number of persons not involved but affected by the FRT system. For the assessment of lawfulness, at least the following should be considered: LED[76], GDPR[77] [78] any existing legal framework on AI[79] and all accompanying guidelines provided by data protection supervisory authorities (such as the EDPB guidelines 3/2019 on processing of personal data

[74] There are different metrics to evaluate the performance of an FRT system. Each metric provides a different view of the system results and its success in providing an adequate picture of whether the FRT system is performing well or not depends on the use case of FRT. If the focus is on achieving high percentages of correct matching a face, metrics such as precision and recall could be used. However, these metrics do not measure how well the FRT handles negative examples (how many were incorrectly matched by the system). The Process Owner, supported by the IT AI and Data Science Department should be able to set the performance requirements and express then in the most suitable metric according to the FRT use case.

[75] Further steps to take care of necessity may be considered as to the tailoring and use of the system, so the description of the use case may also be slightly changed during the necessity and proportionality assessment.

[76] 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.

[77] Regulation (EU) 2016/679 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 and on the free movement of such data.

[78] In cases where a scientific project aiming at researching the use of FRT would need to process personal data, but such processing would not fall under Article 4 (3) LED, generally, the GDPR would be applicable (Article 9(2) LED). In case of pilot projects that would be followed by law enforcement operations, the LED would still be applicable.

[79] For example, there is a proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, however this is not yet established as a regulation.

through video devices[80]). These acts of EU legislation should always be corroborated with the applicable national requirements, especially in the area of criminal procedural law. The proportionality assessment should identify the fundamental rights of data subjects which may be affected (beyond privacy and data protection). It should also describe and consider any limits (or lack of limits) imposed in the use case to the FRT system. For example, if the system will run continuously or temporarily and if it will be limited to a geographical area.

- Perform a Data Protection Impact Assessment (DPIA) [81]. A DPIA should be conducted since the deployment of FRT in the law enforcement area is prone to result in a high risk for the rights and freedoms of the individuals[82]. The DPIA should contain in particular: a general description of the envisaged processing operations[83], an assessment of the risks to the rights and freedoms of data subjects[84], the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance. The DPIA is an ongoing process, so any new elements of the processing should be added and the risk assessment should be updated in each stage of the project.
- Get approval from top management by explaining the risks to the rights and freedoms of data subjects (from the use case and the technology) and the respective risk treatment plans.

3. DURING PROCUREMENT AND BEFORE DEPLOYMENT OF THE FRT

- Decide the criteria to select the FRT (algorithm). The Process Owner should decide the criteria to select an algorithm, with the help of the IT AI and/or Data Science department. In practice, these would include fairness and performance metrics decided in the description of the use case. Such criteria should also include information relating to data the algorithm was trained with. The training, testing and validation set need to sufficiently include samples of all characteristics of data subjects to be subject to the FRT (consider for example, age, gender and race) to reduce bias. The FRT provider should provide information and metrics on the FRT training, testing and validation datasets, and describe the measures taken to measure and mitigate potential unlawful discrimination and bias. The Process Owner, where possible, has to check whether there was a legal basis for the provider to use this dataset for the purpose of the training the algorithms (based on information the provider will make available). Also, the Process Owner should ensure that the FRT provider applies biometric data related security standards, such as ISO/IEC 24745, which provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transmission and

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[81] Further guidance on DPIAs can be found at: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, available at: https://ec.europa.eu/newsroom/article29/items/611236 and the EDPS Accountability on the ground toolkit, part II, available at: https://edps.europa.eu/node/4582_en

[82] FRT, depending on the use case may fall under the following criteria triggering high-risk processing (from Guidelines on DPIA, WP 248 rev.01): Systematic monitoring, data processed on a large scale, matching or combining datasets, innovative use or applying new technological or organizational solutions.

[83] The description of the processing as well as necessity and proportionality assessment as already described in the above steps are also part of the DPIA, apart from risk assessment. If need be, a more detailed description of the personal data flows will be provided in the DPIA.

[84] The analysis of the risks to the data subjects should include risks related to the place of the facial images to be compared (local/remote), risks related to processors/sub-processors, as well as risks specific to machine learning when this is applied (e.g. data poisoning, adversarial examples).

requirements and guidelines for the secure and privacy-compliant management and processing of biometric information.

- Retrain the algorithm (if necessary). The Process Owner should ensure that fine-tuning the FRT system for achieving higher accuracy before its use is also part of the procured services. In case additional training of the acquired FRT system is necessary to meet the accuracy metrics, the Process Owner, apart from taking the decision to retrain, needs to decide, with the help of IT AI and/or Data Science Department on the adequate, representative dataset to be used and check the lawfulness of this use for the data.
- Set the appropriate safeguards to treat risks related to security, bias and low performance. This includes establishing a process to monitor the FRT once in use (logging and feedback for the accuracy and fairness of results). In addition, ensure the risks which are specific to some machine learning and FRT systems (e.g. data poisoning, adversarial examples, model inversion, white-box inference) are identified, measured and mitigated. The Process Owner should also set appropriate safeguards to ensure data retention requirements for biometric data included in the re-training dataset will be respected.
- Document the FRT system. This should include a general description of the FRT system, a detailed description of the elements of the FRT system and of the process for its establishment, detailed information about the monitoring, functioning and control over the FRT system and a detailed description of its risks and mitigation measures. The elements included in this documentation will include main elements of the FRT system description from previous phases (see above), however these will be enhanced with information related to monitoring performance and applying changes to the system, including any version updates and/or re-training.
- Create user manuals, explaining the technology and the use cases. These need to explain all scenarios and prerequisites under which FRT will be used) in a clear manner.
- Train the end users on how to use the technology. Such trainings need to explain the capabilities and limitations of the technology so that the users can understand the circumstances under which it is necessary to apply it and the cases in which it can be inaccurate. Such trainings will also assist in mitigating risks relating to not checking/criticizing the algorithm outcome.
- Consult the data protection supervisory authority, pursuant to Article 28(1)(b) LED. Provide information following Article 13 LED to inform the data subjects about the processing and their rights. These notices need to address the data subjects in appropriate language so that they are able to understand the processing and explain the basic elements of the technology, including accuracy rates, training datasets and measures taken to avoid discrimination and low accuracy of the algorithm.

4. RECOMMENDATIONS AFTER DEPLOYMENT OF THE FRT

- Ensure human intervention and oversight of the results. Never take any measure concerning an individual solely based on the outcome of the FRT (this would imply a breach of Article 11 of the LED- automated individual decision-making having legal or other similar effects on the data subject). Ensure that a LEA officer reviews the results of the FRT. Also ensure that LEA users avoid automation bias, by investigating contradictory information and critically challenging the results of the technology. For this, continuous training and awareness raising to the end users is important, however the top management should ensure there are adequate human resources to perform effective oversight. This entails providing enough time to each agent to critically challenge the results of the technology. Record, measure and assess to which extent the human oversight changes the FRT original decision.
- Monitor and address FRT model drift (performance degradation) once the model is in production.

- Establish a process to re-assess the risks and the security measures regularly and every time the technology or use case suffers any changes.
- Document any change to the system throughout its lifecycle (e.g. upgrades, re-training).
- Establish a process as well as the related technical capabilities to address access requests by the data subjects. Technical capability for the extraction of data, should there be a need to provide them to data subjects, needs to be in place before any request comes up.
- Ensure that there are procedures in place for data breaches. Should a personal data breach occur, involving biometric data, the risks are likely to be high. In this case all involved users should be aware of the relevant procedures to follow, the DPO should immediately be informed and the data subjects be informed.

ANNEX III - PRACTICAL EXAMPLES

There are many different practical settings and purposes of using facial recognition, such as in controlled environments like in border crossings, cross-checking with data from police databases, or from personal data manifestly made public by the data subject, live camera feeds (live facial recognition), etc. As a result, the risks for the protection of personal data and other fundamental rights and freedoms vary significantly in the different use cases. In order to facilitate the necessity and proportionality assessment, which should precede the decision on the possible deployment of facial recognition, the current guidelines provide a non-exhaustive list of possible applications of FRT in the law enforcement field.

The scenarios presented and assessed are based on **hypothetical** situations and are intended to illustrate certain concrete uses of FRT and provide assistance for case-by-case considerations, as well as setting an overall framework. They do not aspire to be exhaustive and are without prejudice to any ongoing or future proceedings undertaken by a national supervisory authority with regard to the design, experimentation or implementation of facial recognition technologies. The presentation of these scenarios should serve only the purpose of exemplifying the guidance to policy makers, legislators and law enforcement authorities, already provided in this document, when devising and envisioning the implementation of facial recognition technologies in order to ensure full compliance with the EU acquis in the field of personal data protection. In this context, it should be borne in mind that even in similar situations of using FRT, the presence, or the absence, of certain elements may lead to a different outcome of the necessity and proportionality assessment.

1 SCENARIO 1

1.1. Description

An Automated Border Control system which allows for an automated border passage by authenticating the biometric image stored in the electronic travel document of EU citizens and other travellers passing the border passage and establishing that the passenger is the rightful holder of the document.

Such verification/authentication involves only one-to-one facial recognition and is carried out in controlled environment (e.g. at airport e-gates). The biometric data of the traveller passing the border passage are captured when he/she is explicitly prompted to look at the camera in the e-gate and is compared to that of the presented document (passport, identity card, etc.) which is issued following specific technical requirements.

At the same time, while the processing in such cases in principle falls outside the scope of the LED, the outcome of the verification may also be used in matching (alphanumeric) data of the person against law enforcement databases as part of the border control and thus may entail actions with significant legal effect for the data subject, e.g. arrest pursuant to an alert in SIS. Under specific circumstances, the biometric data can be also used to search for matches in law enforcement databases (in such a case 1-many identification would be performed in this step).

The outcome of the biometric image processing has a direct impact on the data subject: only in case of successful verification it allows passing the border passage. In case of unsuccessful identification, the border guards need to perform a second check to ensure the data subject is different than the one depicted in the identification document.

In case a SIS or national alert is identified, the border guards need to perform a second verification and the necessary further checks and then take any necessary action, e.g. arrest the person, inform concerned authorities.

Source of information:

- Types of data subjects: ☒ all individuals crossing the borders
- Source of image: ☒ other (ID document)
- Connection to crime: ☒ Not necessary
- Mode of information capture: ☒ in a booth or controlled environment
- Context - affecting other fundamental rights: Yes, namely: ☒ right to free movement ☒ right to asylum

Reference database (to which captured information is compared):

- Specificity: ☒ specific databases related to border control

Algorithm:

- Verification type: ☒ 1-1 verification (authentication)

Outcome:

- Impact ☒ Direct (the data subject is allowed or denied entry)
- Automated decision: ☒ Yes

1.2. Applicable legal framework

Since 2004, pursuant to Council Regulation (EC) No 2252/2004[85], passports and other travel documents issued by Member States have to contain a biometric facial image stored in an electronic chip embedded in the document.

The Schengen Borders Code (SBC)[86] lays down the requirements for border checks on persons at the external borders. For EU citizens and other persons enjoying the right of free movement under Union law, the minimum checks should consist of a verification of their travel documents, where appropriate by using technical devices. The SBC has been subsequently amended with Regulation (EU) 2017/2225[87], which has introduced, *inter alia*, definitions for 'e-gates', 'automated border control system' and 'self-service system', as well as the possibility for processing biometric data for carrying out border checks.

Hence, it could be assumed that there is a clear and foreseeable legal basis authorising this form of personal data processing. Moreover, the legal framework is adopted at Union level and is directly applicable to Member States.

1.3. Necessity and proportionality - purpose/seriousness of crime

Verification of the identity of EU citizens in an automated border control, using their biometric image, is an element of the border checks at the external borders of the EU. Consequently, it is directly related to border security and serves an objective of general interest recognized by the Union. In addition, ABC gates help to speed up the processing of passengers and lessen the risk of human errors. Furthermore, the scope, the extent and the intensity of the interference in this scenario is much more limited compared with other forms of facial recognition. Nevertheless, the processing of biometric data

[85] COUNCIL REGULATION (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.
[86] REGULATION (EU) 2016/399 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).
[87] Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System.

creates additional risks for the data subjects which need to be properly addressed and mitigated by the competent authority deploying and operating the FRT.

1.4. Conclusion

The verification of the identity of EU citizens in the context an automated border control is a necessary and proportionate measure, as long as the appropriate safeguards are in place, in particular the application of the principles of purpose limitation, data quality, transparency and a high level of security.

2 SCENARIO 2

2.1. Description

A system of identification of victims of child abduction is set by the LEAs. An authorised police officer may carry out a comparison of the biometric data of a child, suspected to be abducted, against a database of victims of child abduction under strict conditions, for the sole purpose of identifying minors who may correspond to the description of the missing child for which an investigation has been initiated and the alert issued.

The processing at stake would be the comparison of the face or image of an individual, who may correspond to the description of a missing child, with the images stored in the database. Such processing would happen in specific cases and not on a systematic basis.

The database against which the comparison will be applied is populated with pictures of missing children for which a suspicion of child abduction, a threat to the child's life or physical integrity, has been reported and a criminal investigation has been opened under a judicial authority, and for which an alert for child abduction has been issued. Data are collected within the framework of procedures established by the competent law enforcement authority, that is police officers authorized to carry out judicial police missions. The categories of personal data recorded are:

- identity, nickname, alias, filiation, nationality, addresses, e-mail addresses, telephone numbers;
- date and place of birth;
- parentage information;
- photograph with technical features allowing the use of a facial recognition device and other photographs.

Comparison results must also be reviewed and verified by an authorised officer, in order to corroborate previous evidence with the result of the comparison and rule out any possible false positive results.

Children's pictures and personal data may be retained only for the duration of the alert and must be deleted immediately after the closure or termination of the criminal proceedings in accordance with national procedures for which they have been inserted into the database.

While the retention period for biometric data in the database may be envisioned for a relatively long period of time and defined as per national law, the exercise of data subject rights and in particular the right to rectification and erasure provides for an additional guarantee to limit the interference with the right to the protection of personal data of the data subjects concerned.

Source of information:

- Types of data subjects: ☒ Children
- Source of image ☒ other: not predefined, suspected victim of child abduction
- Connection to crime ☒ Not direct temporal ☒ Not direct geographical
- Mode of information capture: ☒ in a booth or controlled environment
- Context: affecting other fundamental rights ☒ Yes, namely: ☒ various

Reference database (to which captured information is compared):

- Specificity ☒ specific database

Algorithm:

- Verification type: ☒1-many identification

Outcome:

- Impact ☒ Direct
- Automated decision: ☒ NO, mandatory review by an authorized officer

Legal analysis:

- Applicable legal framework: ☒ Specific national law for this processing (facial recognition)

2.2. Applicable legal framework

National law provides for a dedicated legal framework establishing the database, determining the purposes of processing as well as the criteria for the database to be populated, accessed and used. The legislative measures necessary for its implementation also provide for the determination of a retention period as well as referring to the applicable principles of integrity and confidentiality. The legislative measures also foresee the modalities for the provision of information to the data subject and in this case the holder(s) of parental responsibility, as well as the exercise of data subject rights and possible limitation if applicable. During the preparation of the proposal for the respective legislative measure, the national supervisory authority had to be consulted.

2.3. Necessity and proportionality - purpose/seriousness of crime/number of persons not involved but affected by processing

Conditions and safeguards for processing

The facial recognition comparison can only be carried out by an authorised officer as a last resort unless there are no other less intrusive means available and where strictly necessary, for instance, in case there is doubt about the authenticity of a traveling minor's identity document and/or after having reviewed previous evidence and material gathered indicating a possible correspondence with the description of a missing child for which a criminal investigation is being carried out.

An additional safeguard is also provided with the mandatory review and verification of the facial recognition comparison by an authorised officer, in order to corroborate previous evidence with the result of the comparison and rule out any possible false positive results.

Objective pursued

The establishment of the database serves important objectives of general public interest, in particular the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the protection of the rights and freedoms of others. The establishment of the database and the processing foreseen appears to contribute to the identification of children victim of

abduction and therefore can be considered as a measure suitable to support the legitimate objective to investigate and prosecute such crime.

Purpose and population of the database

The purposes of processing are clearly defined by law and the database shall be used only for the purpose of identifying missing children for which a suspicion of child abduction has been reported and a criminal investigation has been initiated under the supervision of a judicial authority and for which an alert for the child abduction has been issued. The conditions set out by law for the population of the database aim at strictly limiting the number of data subjects and personal data to be included in the database. The holder of parental responsibility over the child must be informed about the processing undertaken and the conditions for the exercise of the child's rights in relation to the biometric processing envisioned for the purpose of identification, or to the child personal data stored in the database.

2.4. Conclusion

Considering the necessity and proportionality of the processing envisioned, as well as the best interest of the child in carrying out such personal data processing, and provided that sufficient guarantees are in place to notably ensure the exercise of data subject rights – in particular taking into account the fact that children's data are to be processed, such application of facial recognition processing may be considered as likely compatible with EU law.

Furthermore, given the type of processing and the technology used, which involves a high risk to rights and freedoms of data subject concerned, the EDPB considers that the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to the envisioned processing, must include a prior consultation of the supervisory authority in order to ensure consistency and compliance with the applicable legal framework, cf. Art. 28.2 LED.

3 SCENARIO 3

3.1. Description

In course of police interventions in riots and investigations afterwards, a number of persons have been identified as suspects, e.g. by previous investigations using CCTV coverage or witnesses. Pictures of these suspects are compared with pictures of persons who were recorded on CCTV or mobile devices at a crime scene or in surrounding areas.

In order to obtain more detailed evidence on persons suspected of having participated in riots surrounding a demonstration, the police creates a database consisting of image material with a loose local and temporal connection to the riots. The database includes private recordings uploaded to the police by citizens, material from public transport CCTV, police-owned video surveillance material and material published by the media without any specific limitation or safeguard. The display of severe criminal behaviour is not a prerequisite for the collection of the files in the database. Therefore, persons not involved in the riots – a significant percentage of the local population who happened to pass by at the moment of the demonstration, or participated in the demonstration but not in the riots – are stored in the database. It amounts to thousands of video and image files.

Using a facial recognition software, all faces appearing in those files are assigned to unique face ID's. The faces of individual suspects are then automatically compared to these face ID's. The database consisting of all biometric templates in the thousands of video and images files is stored until all

possible investigations are terminated. Positive matches are dealt with by responsible officers, who then decide on further action. This may include to attribute the file found in the database to the respective person's criminal file as well as further measures, such as questioning or arrest of that person.

A national law provides for a generic provision, according to which the processing of biometric data for the purpose of uniquely identifying a natural person is admissible if strictly necessary and subject to appropriate safeguards for the rights and freedoms of the person concerned.

Source of information:

- Types of data subjects: ☒ all persons
- Source of image: ☒ publicly accessible spaces ☒ private entity ☒ other individuals ☒ other: media
- Connection to crime: ☒ Not necessarily direct geographical or temporal connection
- Mode of information capture: ☒ remote
- Context - affecting other fundamental rights: Yes, namely ☒ freedom of assembly context
- Available additional sources of information about the data subject: ☒ other: not excluded (such as usage of ATM-machines or shops entered), as no control over motives on pictures may be exercised

Reference database (to which captured information is compared):

- Specificity: ☒ specific databases related to crime area

Algorithm:

- Processing type: ☒ 1-many identification

Outcome:

- Impact:☒ Direct (e.g. the data subject may be arrested, questioned)
- Automated decision: ☒ NO
- Duration of storage: until all possible investigations are terminated

Legal analysis:

- Type of prior information to data subject: ☒ In the LEA's website in general
- Applicable legal framework : ☒ LED mostly copied to national law ☒ Generic national law for the use of biometric data by LEAs

3.2. Applicable legal framework

As clarified above, legal bases merely repeating the general clause of Article 10 LED are not sufficiently clear in their terms to give individuals an adequate indication of conditions and circumstances in which LEAs are empowered to use CCTV recordings from public spaces for creating a biometric template of their face and compare it to police databases, other available CCTV or private recordings etc. The legal framework established in this scenario therefore fails to meet the minimum requirements to serve as a legal base.

3.3. Necessity and proportionality

In this example, the processing raises various concerns under the necessity and proportionality principles for several reasons:

Persons are not suspected of a serious crime. The display of severe criminal behaviour is not a prerequisite for the use of the files in the database containing the image material. Also, a direct temporal and geographical connection to the crime is not a prerequisite for the use of the files in the database. This results in a significant percentage of the local population being stored in a biometric database for a duration of potentially several years, until all investigations are terminated.

The crime scene database is not limited to images fulfilling the proportionality requirements, thus leading to an unlimited amount of images to compare. This contradicts the principle of data minimisation. A smaller amount of images would also enable non-algorithmic and less intrusive means to be considered, e.g. super recognizers.[88]

As the example is drawn from surroundings of a protest, it is also likely that images reveal political opinions of participants in the demonstration, being the second special category of data possibly affected in this scenario. In this scenario, it is unclear how the collection of this data can be prevented and with what safeguards. Moreover, when data subjects learn that their participation in a demonstration has resulted in their entry in a biometric police database, this can have serious chilling effects on their future exercise of their right to assembly.

The biometric templates in the database can also be compared with one another. This allows the police not only to look for a specific person in all of their material but also to re-create a person's behavioural pattern over a period of several days. It can also gather additional information on the persons such as social contacts and political involvement.

The interference is further intensified by the fact that the data is processed without the knowledge of the data subjects.

Bearing in mind that photographs and videos are recorded by persons all the time, and that even the omnipresent CCTV-coverage may be analysed biometrically, this can lead to severe chilling effects.

The extensive usage of private photographs and videos, including potential misuse like denunciation, is another point of concern. As misuse like denunciation is a risk also inherent to criminal proceedings in general, the risk is considerably higher as to the scalability of the data processed and the number of the persons involved, as people might upload also material relating to a specific person or group of persons of dislike. Requests by the police to upload photographs and videos possibly lead to very low thresholds for people to provide material, especially as it might be possible to do so anonymously or at least without the need to show up and identify oneself at a police station.

3.4. Conclusion

In the example, there is no specific provision which could serve as a legal base. However, even if there was a sufficient legal base, the necessity and proportionality requirements would not be met, thus resulting in a disproportionate interference with the data subject's rights to respect for private life and the protection of personal data under the Charter.

[88] I.e. people with extraordinary face-recognition ability. Cf. also: Face Recognition by Metropolitan Police Super-Recognisers, 2016 Feb 26, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

4 SCENARIO 4

4.1. Description

The police implements a way of identifying suspects committing a serious crime caught on CCTV by retrospective FRT. An officer manually selects image(s) of suspects in the video material that has been collected from the crime scene or elsewhere within a preliminary investigation and then sends the image(s) to the forensic department. The forensic department uses FRT to match these image(s) to pictures of individuals that have previously been gathered in a database by the police (a so called description database that consists of suspects and former convicts). The description database is for this procedure – temporarily and in an isolated environment – analysed with FRT in order to be able to carry out the matching process. To minimize the interference with the rights and interests of the persons matched, a very limited number of employees at the forensic department have permission to conduct the actual matching procedure, access to the data is restricted to those officers entrusted with the specific file and a manual control of the results is carried out before forwarding any result to the investigating officer. The biometric data is not forwarded outside of the controlled, isolated environment. Solely the result and the picture (not biometric template) is further used in the investigation. Employees receive specific training on the rules and procedures for this processing and all processing of personal and biometric data is sufficiently specified in national law.

Source of information:

- Types of data subjects: ☒ suspects identified from the CCTV recordings
- Source of image: ☒ publicly accessible spaces ☒ internet
- Connection to crime: ☒ Direct temporal
  ☒ Direct geographical
- Mode of information capture: ☒ remote
- Context - affecting other fundamental rights: Yes, namely : ☒ Freedom of assembly ☒ Freedom of speech ☒ various: __

Reference database (to which captured information is compared):

- Specificity: ☒ specific databases related to crime area

Algorithm:

- Processing type: ☒ 1-many identification

Outcome:

- Impact:☒ Direct (e.g. the data subject is arrested, questioned)
- Automated decision: ☒ NO

Legal analysis:

- Applicable legal framework : ☒ Specific national law for this processing (facial recognition) for that competent authority

4.2. Applicable legal framework

In this scenario, it is specified in national law that biometric data may be used in conducting forensic analysis when strictly necessary for achieving the purpose of identifying suspects committing a serious crime through the matching of the pictures in the description database. The national law specifies which data that may be processed, as well as the procedures for preserving the integrity and

confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

4.3. Necessity and proportionality

The use of facial recognition is clearly more time efficient than manual matching at the forensic level. The manual selection of images beforehand limits the interference compared to running all the video material against a database and thereby differentiates and targets only those persons covered by the objective, i.e. fighting serious crime. It is however still important to consider whether the matching can be done manually within a reasonable amount of time, depending on the case at hand. The restriction of persons with access to the technology and the personal data lessens the impact on the rights to privacy and data protection, as well as the biometric templates not being stored or used later on in the investigation. The manual control of the result also means a reduced risk of any false positives.

4.4. Conclusion

It is important that national legislation provides an adequate legal basis for the processing of biometric data as well as for the national data base to which the matching takes place. In this scenario several measures have been put in place in order to limit the interference with data protection rights, such as the conditions for the use of the FRT specified in the legal basis, the number of people with access to the technology and the biometric data, manual controls etc. The FRT significantly improves efficiency in the investigatory work of the forensic department of the police, is based on law allowing for the police to process biometric data when absolutely necessary and therefore, within these perimeters may be considered a lawful interference of the rights of the individual.

5 SCENARIO 5

5.1. Description

Remote biometric identification is when the identities of persons are established with the help of biometric identifiers (facial image, gait, iris, etc.) at a distance, in a public space and in a continuous or ongoing manner by checking them against (biometric) data stored in a database[89]. Remote biometric identification is conducted in real-time, if the capturing of the image material, the comparison and the identification happen with no significant delay.

Prior to each deployment of real time remote biometric identification, the police compiles a watch list of subjects of interest as part of an investigation. It is populated with facial images of the individuals. Based on intelligence suggesting that the individuals will be in a specific area, such as a shopping mall or a public square, the police decides when, where and for how long to deploy the remote biometric identification.

On the action day, they place a police van on the ground as a control centre, with a senior police officer on board. The van contains monitors displaying footage from CCTV cameras sited nearby, either installed on an ad-hoc basis or by connecting to the video streams of cameras already installed. As pedestrians pass by the cameras, the technology isolates facial images, converts them to a biometric template and compares these to the biometric templates of those on the watch list.

If a potential match between the watch list and those passing the cameras is detected, an alert is sent to officers in the van, who then advise officers on the ground if the alert is positive, e.g. via radio device. The officer on the ground will then decide whether to intervene, approach or ultimately apprehend

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

the individual. The measures taken by the officer on the ground are recorded. In the case of a discreet check, the information gathered (such as who the person is with, what they are wearing and where they are heading to) is stored.

A national law referred to provides for a generic provision, according to which the processing of biometric data for the purpose of uniquely identifying a natural person is admissible if strictly necessary and subject to appropriate safeguards for the rights and freedoms of the person concerned.

Source of information:

- Types of data subjects: ☒ all persons
- Source of image: ☒ publicly accessible spaces
- Connection to crime: ☒ Not necessarily direct geographical or temporal connection
- Mode of information capture: ☒ remote
- Context - affecting other fundamental rights: Yes, namely: ☒ Freedom of assembly ☒ Freedom of speech ☒ various
- Available additional sources of information about the data subject: ☒ other: not excluded (such as usage of ATM-machines or shops entered)

Reference database (to which captured information is compared):

- Specificity: ☒ specific databases related to crime area

Algorithm:

- Processing type: ☒ 1-many identification

Outcome:

- Impact:☒ Direct (e.g. the data subject is arrested, questioned)
- Automated decision: ☒ NO
- Duration of storage: until all possible investigations are terminated

Legal analysis:

- Type of prior information to data subject: ☒ In the LEA's website in general
- Applicable legal framework: ☒ LED mostly copied to national law ☒ Generic national law for the use of biometric data by LEAs

5.2. Applicable legal framework

Legal bases merely repeating the general clause of Article 10 LED are not sufficiently clear in their terms to give individuals an adequate indication of conditions and circumstances in which LEAs are empowered to use CCTV recordings from public spaces for creating a biometric template of their face and compare it to police databases. The legal framework established in this scenario therefore fails to meet the minimum requirements to serve as a legal base. [90]

5.3. Necessity and proportionality

The bar for necessity and proportionality becomes higher the deeper the interference. There are several fundamental rights implications of remote biometric identification in public spaces:

[90] In cases where a scientific project aiming at researching the use of FRT would need to process personal data, but such processing would not fall under Article 4 (3) LED or outside the scope of Union law, the GDPR would be applicable. In case of pilot projects that would be followed by law enforcement operations, the LED would still be applicable.

The scenarios entail the monitoring of every passers-by in the respective public space. Thus, it severely affects the populations' reasonable expectation of being anonymous in public spaces[91]. This is a prerequisite for many facets of the democratic process, such as the decision to join a civic association, visit gatherings and meet people of all social and cultural backgrounds, participate in a political protest and visit places of all kinds. The notion of anonymity in public spaces is essential to gather and exchange information and ideas freely. It preserves the plurality of opinion, the freedom of peaceful assembly and freedom of association and the protection of minorities and supports the principles of separation of powers and checks and balances. Undermining the notion of anonymity in public spaces can result in a severe chilling effect on citizens. They may refrain from certain behaviours which are well within the remits of a free and open society. This would affect the public interest, as a democratic society requires the self-determination and participation of its citizens in the democratic process.

If such a technology is applied, simply to walk on the street, to the subway or to the bakery in the affected area will lead to the collection of personal, including biometric data by law enforcement agencies and, in the first scenario, also to matching with police databases. A situation, where the same would be done by taking fingerprints, would be clearly disproportionate.

The number of data subjects affected is extremely high, since everyone walking past the respective public area is affected. Furthermore, the scenarios would imply automated mass processing of biometric data, and also a mass matching of biometric data against police databases.

Across European case law, mass surveillance is prohibited (e.g. the ECtHR in S. and Marper v UK considered the indiscriminate retention of biometric data as a "disproportionate interference" with the right to privacy, as it fails to be regarded "necessary in a democratic society").

Remote biometric identification is so prone to mass surveillance that there are no reliable means of restriction. It is essentially different from video surveillance as such, as the possible use of video footage without biometric identification is already a strong interference, but at the same time limited, whereas if FRT is applied, the already wide-spread video surveillance system as the main source of the data will undergo a change of quality. Moreover, especially with regard to the chilling effects implied, possible restrictions in the application of the already existing video surveillance installations will not be visible and thus not trusted by the public.

Remote biometric identification by police authorities treats everyone as a potential suspect. In a state under the rule of law, however, citizens are presumed to be righteous until misconduct can be proven. This principle is also partly reflected in the LED, which underlines the need for distinction, in so far as possible, between the treatment of criminal convicts or suspects in which case law enforcement must have "*serious grounds for believing that they have committed or are about to commit a criminal offence*" (Article 6(a) LED) compared to those who are not convicted or suspected of criminal activity.

Applied to transport nodal points or public spaces, with law enforcement agencies using a technology able to uniquely identify a single person, and to trace and analyse its whereabouts and movements will reveal up to the most sensitive information about a person (even sexual preferences, religion, health problems). With this comes the immense risk of unlawful access and use of the data.

The installation of a system that enables uncovering the very core of the individual's behaviour and characteristics leads to strong chilling effects. It makes people question whether to join a certain manifestation, thus damaging the democratic process. Also meeting and being seen in public with a

[91] EDPB response to MEPs, concerning the facial recognition app developed by Clearview AI, 10 June 2020, Ref: OUT2020-0052.

certain friend known as having trouble with police or behaving in a unique way might be seen as critical, since all of this would lead to the attraction of the system's algorithm and thus of law enforcement.

It is impossible to protect vulnerable data subjects like children. Moreover, persons who have a professional interest in – and often a corresponding legal obligation to – keeping their contacts confidential, such as journalists, lawyers and clergy, are affected. This could e.g. lead to the revelation of the source and the journalist, or the fact that a person consults a criminal defence attorney. The problem does not only apply to random public places, where e.g. journalists and their sources meet, but naturally also to public spaces necessary to approach and access institutions or professionals in this regard.

Furthermore, people's discomfort with FRT may lead them to changing their behaviour, avoiding places where FRT is deployed and thus withdrawing from social life and cultural events. Depending on the extent of the FRT deployment, the impact on people may be so significant as to affect their capacity to live a dignified life[92].

Therefore, there is a strong likelihood to affect the essence – the untouchable core – of the right to protection of personal data. Strong indications (cf. section 3.1.3.2 of the guidelines) are in particular the following: on a large scale, people's unique biological features are automatically processed by law enforcement authorities with algorithms based on plausibility with only a limited explainability of the results. The limitations to the rights to privacy and data protection are imposed irrespective of the person's individual conduct or the circumstances concerning him or her. Statistically almost all of the data subjects affected by this interference are law-abiding individuals. There are only limited possibilities of providing information to the data subject. Judicial recourse in most cases will only be possible subsequently.

The reliance on a system based on plausibility and with limited explainability may lead to diffusion of liability and a lack in the field of remedy and may be an incentive towards negligence.

Once such a system, that may be applied also to existing CCTV cameras, is applied, with very little effort and without being visible to the individuals, it may be misused and enabled to systematically and speedily draw up lists of people according to ethnic origin, sex, religion etc. The principle of processing personal data against pre-determined criteria such as a person's whereabouts and the route travelled is already practiced[93] and is prone to discrimination.

Corresponding to the sensitivity, the expressiveness and the quantity of data processed, systems for remote facial recognition in publicly accessible places are prone to be misused with detrimental effects for the concerned individuals. Such data may also be easily collected and misused to put pressure on key actors in the principle of checks and balances such as political opposition, officers and journalists.

---

[92] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, page 20.

[93] C.f. Article 6 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime and Article 33 Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.

Lastly, FRT-systems tend to incorporate strong bias effects regarding race and gender: false-positive results disproportionately affect people of colour and women[94], resulting in discrimination. Police measures following a false-positive result, such as searches and arrests, stigmatise these groups further.

5.4. Conclusion

The aforementioned scenarios concerning remote processing of biometric data in public spaces for identification purposes fail to strike a fair balance between the competing private and public interests, thus constituting a disproportionate interference with the data subject's rights under Articles 7 and 8 of the Charter.

6 SCENARIO 6

6.1. Description

A private entity provides an application where facial images are scraped off the internet to create a database. The user, e.g. the police, can then upload a picture and by using biometric identification the application will try to match it with the facial images or biometric templates in its database.

A local police department is conducting an investigation of a crime caught on video where a number of potential witnesses and suspects cannot be identified through matching collected information with any internal databases or intelligence. The individuals are, based on the information collected, not registered in any existing police database. The police decides to use a tool as described above, which is provided by a private company, to identify the individuals through biometric identification.

Source of information:

- Types of data subjects: ☒ all citizens (witnesses) ☒ convicts ☒ suspects
- Source of image: ☒ Video footage from a public place or collected elsewhere within a preliminary investigation
- Connection to crime: ☒ Not necessary
- Mode of information capture: ☒ remote
- Context - affecting other fundamental rights: Yes, namely: ☒ Freedom of assembly ☒ Freedom of speech ☒ various: __

Reference database (to which captured information is compared):

- Specificity: ☒ general purpose databases populated from internet

Algorithm:

- Processing type: ☒ 1 - many identification

Outcome:

- Impact ☒ Direct (e.g. the data subject is arrested, questioned, discriminatory behavior)
- Automated decision: ☒ NO

Legal analysis:

- Type of prior information to data subject: ☒ No

[94] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

6.2. Applicable legal framework

When a private entity provides a service that includes personal data processing for which they determine the purpose and means (in this case scraping images off the internet to create a database), this private entity must have a legal basis for this processing. Furthermore, the law enforcement authority that decides to use this service for their purposes must have a legal basis for the processing for which they determine the purposes and means. For the law enforcement authority to be able to process biometric data, there has to be a legal framework that specifies the objective, the personal data to be processed, the purposes of the processing and the procedures for preserving the integrity and confidentiality of personal data as well as procedures for its destruction.

This scenario implies mass-scale collection of personal data from individuals not aware of their data being collected. Such processing could be lawful only under very exceptional circumstances. Depending on where the database is located using such a service may entail transferring personal data and/or special categories of personal data outside the European Union (by the police, e.g. "sending" the facial image in the surveillance video or collected otherwise), thereby requiring specific conditions for that transfer, see Article 39 LED.

There are no specific rules in this scenario that allow this processing by the law enforcement authority.

6.3. Necessity and proportionality

The law enforcement authority's use of the service means that personal data is shared with a private entity that is using a database where personal data is collected in an unlimited, mass-scale way. There is no connection between the personal data collected and the pursued objective by the law enforcement authority. The sharing of data by the law enforcement authority to the private entity also means a lack of control for the authority over the data being processed by the private entity and great difficulty for data subjects to exercise their rights, as they will not be aware of their data being processed in this way. This sets a very high bar for situations when such a processing could even take place. It is questionable if any objective would meet the requirements set out in the Directive, since any derogations from, and limitations to, the rights to privacy and data protection are only applicable when strictly necessary. The general interest of effectiveness in fighting serious crimes cannot in itself justify processing where such vast amounts of data are being collected indiscriminately. This processing would therefore not meet the requirements for necessity and proportionality.

6.4. Conclusion

The lack of clear, precise and foreseeable rules that meet the requirements in Articles 4 and 10 of the Directive, and the lack of evidence that this processing is strictly necessary in order to achieve the intended objectives, leads to the conclusion that the use of this application would not meet the necessity and proportionality requirements and would mean a disproportionate interference of data subjects' rights to respect for private life and the protection of personal data under the Charter.