Written observations by the Ministry of Justice and Security and the Ministry of Defence, on the draft-Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement

The Ministries would like to bring the following comments to the attention of the European Data Protection Board.

- 1. Some principles relating to the processing of personal data (article 4 LED) are addressed in great detail which is very useful. Given that FRT processing must comply with all principles, the Ministries would appreciate some additional explanation on how to apply the principles which are currently briefly mentioned in the guidelines. This would include, for example, the principles of data minimisation, accuracy (margin of error, data quality, etc) and storage limitation.
- 2. Annex III of the guidelines provides many practical scenarios that are of great added value for the practical use of the guidelines. The Ministries would like to advise to provide additional elaborations and practical explanations whether a FRT processing meets the requirements of (strict) necessity, proportionality, subsidiarity and the other principles relating to the processing of personal data (article 4 LED). For example, in scenario 1 and scenario 4. This would further enhance the practical use of the guidelines.
- 3. Section 30 of the guidelines rightfully mentions the need for data controllers to undertake regular evaluation of algorithmic processing in order to ensure the accuracy, fairness and reliability of FRT. However to fulfill that obligation, largescale additional processing of biometric personal data may be required in order to adequately evaluate and improve the technology. It would be highly valuable if the guidelines could further elaborate on ways data controllers can meet this obligation while at the same time not contradicting other privacy principles such as purpose limitation and data minimisation.
- 4. The guidelines elaborate in detail on the rights of data subjects and in particular on providing information to the data subject. However, the nature and context of FRT processing often means that data controllers especially LEA's need to restrict the obligation to provide information to the data subject. For example, during an ongoing police investigation. This is briefly mentioned in section 88 of the guidelines. The Ministries advise to address this topic in more detail and provide additional explanation, perhaps illustrated with an example.
- 5. In the context of security measures, section 100 provides specific (logging) measures that are recommended when using FRT. The Ministries find this very practical. Therefore, the Ministries would like to suggest to also provide various examples of measures that would be recommended for an organization using FRT in section 98 and 99.
- 6. Finally, to enhance the practical use and clarity of the annexes the Ministries suggest to add a brief introduction to Annex I with an explanation and clarification of the terms used. The Ministries would also recommend to emphasize in the introduction of Annex II that, although it provides a sound basis for the management of a FRT project, there is no "one size fits all" and it is important LEA's take into account their own organizational structures and working procedures.

Joint Response of the Dutch Police and Dutch Prosecution to the EDPB FRT guidelines

The Dutch Police and the Dutch Prosecution (DP-DP hereafter) have studied the Draft Guidelines for Facial Recognition by European Data Protection Board (EDPB hereafter) with great interest and wish to make use of the invitation to comment on these guidelines.

DP-DP are pleased to find that many of the risks and recommendations contained in these draft guidelines are familiar since the Dutch Police has been engaged in the process of drafting guidelines for the use of facial recognition of their own since 2020. These guidelines are now in the final stages of completion and will be presented to the Minister of Justice and Security (Minister hereafter) and the Dutch House of Representatives (the House hereafter) shortly.

This drafting process was initiated in response to the letter of the Minister to the House in November 2019. 1 Here the Minister addressed worries regarding the use of FRT in Dutch society. The Minister effectively forbade any operational use of facial recognition until proper legal and ethical deliberation could be shown to have taken place. This resulted in the creation of a Community on Facial Recognition in which over a hundred people from both inside and outside the Dutch Police have participated.

A year was spend on discussing different concepts and all the technical, legal and ethical issues that might occur in the real life application of them. This was done with the sole purpose of gathering information to write a guideline that would cover specific and overarching risks and yet be specific enough to guide law enforcement in the creation of the prospective plans that could pass stringent checks. The results of these discussions were taken as input for the writing of the Guidelines for operational use of FRT (Inzetkader Gezichtsherkenning).

DP-DP appreciate the work done by the EDPB and have several observations that they would like to share with the EDPB in response to these Concept Guidelines.

General remarks

- DP-DP feel that while great effort was clearly put in this document it is slightly over focused on data and privacy protection. More space could have been spent in recognizing possible applications of FRT that are beneficial to society in general and could stand even stringent privacy tests, resulting in a more balanced guideline to be used in practice.

DP-DP take the position that understaffing or efficiency concerns should never on their own be a reason to employ technology that can (unduly) infringe on privacy. However, while recognizing the potential dangers of the use of FRT, they wish to emphasize that use cases are indeed imaginable where the use of FRT may improve the quality of police work and judicial procedures and may in fact prevent the use of other measures to attain similar goals that might infringe more on citizen's privacy and autonomy or disrupt public life. This of course taking into account the different focus in different areas of law enforcement.

In this regard DP-DP recognize the potential value of providing use-cases, but in their opinion they are not specific and detailed enough. To be truly helpful for practice DP-DP feel they should be

¹ Grapperhaus, F.J.B. (Minister of Justice and Security), 'Waarborgen en kaders bij gebruik gezichtsherkenningstechnologie', Letter to the Chair of the House of Representatives, November 20th, 2019

² An exemption was made for the version of Catch running in November 2019 as the Minister felt adequate safeguards and procedures existed there.

further fleshed out and more attention given to different application possibilities of FRT compared to the privacy infringement risks.

- DP-DP wish to make clear that they are well aware of the potential chilling effect of the possibility of the use of FRT everywhere, especially when citizens cannot determine when and where they are (possibly) subjected to it. Therefore the Dutch police will make their own Guidelines for operational implementation of FRT available to everyone.
- DP-DP would like to point out that not all usage of FRT leads to legal decisions as intended in the GDPR and LED. For example FRT could be used to identify victims in order to help the investigation into their case.
- DP-DP are of the opinion that a number of the terms used in these guidelines require clarification in order to be truly useful in practice and realizes this will likely have to be done in the AI regulation currently being negotiated. The Dutch police and Dutch prosecution have provided feedback in the course of this process several times. Unfortunately, much is still unclear about terms such as 'remote' and 'publicly accessible spaces'. The impression remains that different parties may mean different things when using such terms. Especially where the AI regulation aims to regulate both private and public parties in one regulation DP-DP would like to point out that specific regulation relevant for law enforcement such as implemented in the GDPR and the Directive 2016/680 (LED) is preferable as law enforcement has specific areas of application as well as a context specific to them. As long as the actual concerns behind the wording remain unclear it is very hard to effectively address them. This should be addressed in further drafts of the EU 'AI regulation' and a future version of these guidelines.

Specific remarks

- These Guidelines differentiate between the use of FRT of authentication and identification of a person. However, later in these guidelines the use of FRT for 'categorisation' is also addressed. DP-DP believe that such use of FRT does not fall under either of these and should be considered separately. DP-DP wish to take the opportunity to express their opinion that the use of FRT for categorization of discriminatory nature is in fact already not legally possible.

However, not every singular use of certain characteristics is discriminatory in nature, as article 11 of the LED allows for. As such a full ban is inadvisable as it would hamper law enforcement effectiveness and might lead to measures applied to unrelated citizens on a larger scale than necessary. DP-DP do feel that any use of such criteria should pass even higher standards that the use of FRT in general already should.

- DP-DP are of the opinion that a clear distinction ought to be made between 'facial recognition' and the 'detection of faces'. The latter is much less invasive and uses or stores no biometric profiles.
- The EDPB Guidelines, whether intended or not, focusses overmuch on systems created by (private) industry and their procurement, while these are not a necessary given. DP-DP feel that the guidelines should reflect the possibility of non-commercial parties developing such systems themselves in part or in whole, therefore having intimate knowledge of and control over their internal workings. This would for instance enable law enforcement to avoid systems that have been made or trained on the large scale scraping of the internet for faces for training material. This however, does require that some form of data collection and the use of it be allowed in some form (preferably by independent

parties such as for instance NIST) as systems cannot be trained and improved without it. DP-DP would look forward to further discussions of this.

- DP-DP feel that in public discussions too much weight is given only to the options of outright deletion of data or the technical measure of blurring. While irreversible blurring will in some cases be a proper measure, in other cases situations specific to law enforcement in general and Dutch law specifically will require the forensically sound unaltered safekeeping of original materials. In such cases other measures than blurring ought to (be allowed to) be employed to reach the required level of privacy protection and data minimalisation, whilst keeping the original materials available.
- While DP-DP in principle support logging as a tool in a larger toolbox for compliance and supervision experience has learned that simply implementing logging simply creates data. It is the use that is made of that data in combination with proper procedures that will make it useful. A balanced procedure for assessing the use of FRT in operational cases should always result in both procedural checks and constant monitoring of the quality of execution, in which logging may and should take a role. DP-DP are both already implementing policies and measures to enforce these internal checks and balances at the national level.
- DP-DP oppose decision-making in law enforcement based solely on the use of FRT. As a matter of principle any use of FRT should always include a meaningful human-in-the-loop. DP-DP are also of the opinion that using FRT as the sole basis for automated decision making might be in violation of the GDPR and the LED.
- DP-DP feel that not enough proper scientific research exists to show that emotion detection is effective or reliable with or without the use of FRT. DP-DP are therefore of the opinion that FRT should not currently be used for such purposes.
- While DPIA's ought to be standard-procedure for any system with significant risks of infringing privacy DP-DP wish to emphasize that it is both impossible and unnecessary to go through a DPIA every single time technology is applied in the execution of law enforcement tasks. Protective measures already exist in the relevant laws and regulations and national policies of DP-DP.

In general DP-DP wish to remark that policy on when exactly and how often a DPIA is required is a matter of ongoing discussions. Additionally, DP-DP support the general idea of public DPIA's but must emphasize that specifically in law enforcement valid reasons might exist to share the outcomes of such a process only with for instance a supervisory authority, not the public at large.

- DP-DP feels that the guidelines in the aspect of informing persons submitted to the use of FRT are too general and do not take the specifics of law enforcement into account. They believe that a solution and exceptions similar to those stated in article 23 GDPR should be implemented to ensure investigative interests.

In conclusion DP-DP wish to express their gratitude for the work done by the EDPB; The Community on Facial Recognition (Community Gezichtsherkenning) would like to take this opportunity to formally invite representatives of the EDPB to discuss our Guidelines for operational implementation of FRT once they are completed and made public.