Centre for Information Policy Leadership
Hunton Andrews Kurth

6 September 2019

CENTRE FOR INFORMATION POLICY LEADERSHIP RESPONSE

CONSULTATION BY THE EUROPEAN DATA PROTECTION BOARD ON GUIDELINES 3/2019 ON PROCESSING OF PERSONAL DATA THROUGH VIDEO DEVICES

On 10 July 2019, the European Data Protection Board (EDPB) adopted its Draft Guidelines 3/2019 on processing of personal data through video devices (Draft Guidelines or Guidelines).[1] The EDPB invited public comments on this document by 9 September 2019.

The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit the comments below as input for the EDPB's final Guidelines (Final Guidelines).

This paper (Paper) contains two sections. The first section provides comments on the use of video devices generally and the second section focuses exclusively on paragraphs 5.1 and 5.2 of the Guidelines which relate more specifically to facial recognition.

I. General comments on the use of video devices

CIPL wishes to highlight that video devices and in particular CCTV—whether or not they process personal data—have been widely used for several decades, in particular for safety and security reasons, and have proven their effectiveness. Video devices are generally used for legitimate purposes such as protecting citizens in their homes and communities, employees in a building or workers on a construction site. Video devices may also help to secure critical assets of public and private organisations such as warehouses, plants, labs or restricted and confidential R&D areas.

Videoconferencing tools are also widely used by organisations, their employees and stakeholders for the purpose of internal and external communications. Although videoconferencing tools are not specifically mentioned by the Draft Guidelines, CIPL would welcome clarification from the EDPB that they are out of the scope of the Guidelines.

[1] Draft Guidelines 3/2019 on processing of personal data through video devices, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 77 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

6 September 2019

CIPL welcomes the confirmation by the EDPB that any legal ground under Article 6(1) of the GDPR can provide a legal basis for processing personal data through video devices, and that legitimate interest is the preferred legal basis for such processing. The Guidelines provide that consent may be used only in exceptional cases. CIPL agrees that consent may not be an appropriate legal basis due in particular to the difficulty of obtaining consent in a physical setting. Consistent with CIPL's previous work on this topic,[3] CIPL confirms that consent needs to be reserved for contexts where individuals can make meaningful choices about the processing of their personal data. Reliance on legitimate interest does not weaken the protection of individuals, as it still requires the controller to perform a documented balancing test and to put in place the appropriate mitigations and accountability measures, including those enabling the exercise of data subject rights.

CIPL regrets however that the Guidelines adopt a restrictive approach that is not always aligned with organisations' use of video devices, particularly in the analysis of the controller's legitimate interests, the processing of special categories of data, rights of data subjects and the obligation of transparency.

Legitimate interest, necessity of the processing and balancing of interests

The Guidelines appear to set the legitimate interest bar so high that it would have the effect of unreasonably restricting the use of video devices.

- The Guidelines fail to recognise the overall benefits that video devices and related data processing can bring to both data subjects and controllers (e.g. lower-cost security systems, less intrusive implementations of monitoring—e.g. passive video systems instead of an in-person security guard—and beneficial public safety use cases). These benefits are a critical aspect that controllers should take into account during the assessment of the legitimate interest in order to balance the interests at stake. For instance, when assessing whether alternative solutions would have equally achieved the purpose of protecting a building or a restricted area, the controller should consider the cost, accuracy and efficiency of the video processing compared to available alternatives (e.g. physical security guards, lights, fences, etc.).

- **Paragraph 20** of the Guidelines appears disproportionate in its interpretation of the standard required under the GDPR for a legitimate interest by requiring a real and present situation of distress to legitimise the use of video devices. It does not appear realistic that an organisation, especially a small business (or even a homeowner), needs to collate empirical and localised evidence of past incidents before deploying a CCTV system. CCTV has been a fact of retail environments for a long time and shoplifting, vandalism, abuse of staff, etc. are recognised risks and concerns. This requirement poses a disproportionate and unnecessary burden while not considering the protection that such devices bring to the organisation, its employees and clients and their proactive dissuasive effects on misbehaviours. The controller's efforts would be better

[3] See Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Consent" adopted on 28 November 2017. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_guidelines_on_consent-c.pdf

placed ensuring the CCTV system itself is implemented in a manner that respects the data protection principles of the GDPR, such as for instance data minimisation, storage limitation or confidentiality.

- Similarly, the Guidelines' proposed weighing of the data controller's and data subject interests' seems unreasonable and unrealistic. The Guidelines refer in **paragraphs 32** and **33** to the "*intensity of the intervention for the right and freedom of the individual*" as a decisive criterion of the balancing of interests. Such new criterion is unclear and adds unnecessary complexity to the performance of the well-known "balancing test" required under Article 6(1)(f) of the GDPR. For instance, the number of data subjects concerned may not be relevant. There is generally no relation between the number of people monitored (e.g. an identical CCTV system used for a store where only 50-plus people enter a day versus a store where more than 5,000 people a day enter) and the impact this may have on an individual's data protection rights.

- The dash cam example in **paragraph 34** of the Guidelines appears to suggest that a dash cam will only be lawful if the technology includes "adverse event triggers" (whereby it only begins recording on impact), whereas by their very nature, accidents are unpredictable. By recommending that the camera should not constantly record traffic, this approach fails to recognise the enormous value of dash cams in protecting drivers, cyclists and pedestrians. The "adverse event triggers" do not currently exist for most video systems and even if such systems were implemented as described in this example, then the dash cam would only capture data after the event, not what precipitated the accident, thus limiting the system's effectiveness. CIPL would suggest that this example be clarified to mean that traffic should not be recorded when the vehicle is not in use. In addition, the Guidelines should emphasise the need to respect the data protection principles of the GDPR such as data minimisation (selective field of vision, for example), retention periods according to the purpose of the processing, security, etc.

- The Guidelines outline that the assessment of legitimate interest should include the reasonable expectations of privacy of the data subject, based on an objective third-party criterion. The use of a third-party criterion for an individual data subject's expectation of privacy is uncommon, as previously reasonable expectations of privacy have been considered on a case-by-case basis with a totality of factors considered. The example in **paragraph 36** suggests that an employee in his/her workplace is in most cases not likely expecting to be monitored by his or her employer. However, employees' reasonable expectation largely depends on the type of workplace. While constant monitoring of a fixed work desk may not be acceptable, other types of "workplaces" (e.g. security guards walking through a building with cameras, receptionists accompanying visitors to meeting rooms and crossing areas with CCTV, fulfilment employees walking around a building with CCTV areas, etc.) may justify non-permanent monitoring of the respective employees. Further, a data subject who freely enters into a premise with clear notices about video surveillance cannot have a reasonable expectation of privacy in the public areas of those premises.

- At **paragraph 37**, the Guidelines suggest that data subjects should not be monitored during leisure activities and in recreation areas, such as in public sitting areas, restaurants, parks, cinemas, etc. CIPL recommends that the Guidelines do not provide for such a sweeping statement, as the

balance of interests in these contexts may support a very clear legitimate interest in video monitoring in these areas, such as to protect the safety and security of those who want to use them lawfully. Further, some of these spaces—like cinemas—may be privately owned, meaning the property owner should be in the best position to make a case-by-case determination on the legitimate interest of any video-processing efforts. Some of these areas may actually face high instances of crime, particularly petty theft (pickpocketing), vandalism, assaults, etc. More generally CIPL wishes to highlight that data subjects' expectations are evolving since dependent on the uses and customs and the societal challenges. For instance, the current expectations regarding video surveillance at work, in airports, in the streets, in football stadiums, in shopping centres, etc. are not the same as those that we had 10 years ago. In addition, in certain EEA jurisdictions, video surveillance systems are used in museums, banks, jewellery stores, etc. Finally, evolving societal demands must also be taken into account, such as video surveillance to protect children (e.g. in kindergarten) and face detection or recognition technology being deployed as commonplace (e.g. in airports).

- CIPL believes that the wording of **paragraph 39** of the Guidelines is unclear. The statement on the lack of relevance between the signs informing the data subjects about video surveillance and what data subjects can reasonably expect should be clarified or removed. If the balancing of interests affirms an appropriate reliance on the legitimate interest legal basis and if there is transparency to data subjects that video recording is in operation in a particular area they are entering (i.e. data subjects have been informed by signs), data subjects should be deemed to be in a position to "objectively expect" video surveillance.

- CIPL suggests that the example provided in **paragraph 45** be reviewed. In its current state, it considers that entering a marked monitored area through a special entrance would not constitute a statement or a clear affirmative action that would serve as valid consent. CIPL considers however that if the information provided to the data subjects before they enter such area is sufficiently clear and otherwise complies with Article 7 of the GDPR, it may serve as confirming consent under the GDPR. The GDPR requires that the consent consist of a statement or clear affirmative act. To engage in an active behaviour (i.e. entering into a video-surveilled place after having been informed of the consequences of this behaviour—i.e. to be recorded for a specific purpose) is an explicit and affirmative indication of a will. It also constitutes a practical and pragmatic approach to obtaining consent at events or activities where video devices are being used.

More generally, instead of focusing on restricting the use of video recording, given the wide use of video devices, the Guidelines should instead provide more practical examples relying on existing practices on how to conduct the operation of the video device in an accountable manner. This could mean for instance ensuring proper security and performing regular audits.

6 September 2019

Summary of CIPL Recommendations:

- Clarify that videoconferencing tools are outside of the scope of the Guidelines.

- Recognise the overall benefits of video devices to data subjects and controllers and their role in the legitimate interest balancing test.

- Lower the bar of the balance interest test to legitimise the use of video devices for security and safety purposes.

- Clarify the dash cam example to mean that traffic should not be recorded when the vehicle is not in use.

- Avoid broad statements that video devices should not be used in specific cases and consider data subjects' evolving expectations as well as the specific context.

- Amend example in paragraph 45 to confirm that entering a clearly marked monitored area constitutes valid consent.

Processing of special categories of data

The Guidelines describe the circumstances where data processed through video devices will not be considered as special categories of data unless they are processed to "deduce" data that fall under special categories of data under the GDPR. CIPL believes that the Guidelines should include a more fulsome explanation of what this means in practice and adapt the corresponding examples. Example 12 in **paragraph 63** in particular explains that political opinions could be deduced from images showing identifiable data subjects taking part in an event or engaging in a strike. CIPL considers in this instance that the images of the event should only be considered as special categories of data if the controller actually uses the footage to deduce or infer the participant's political opinions. The fact that it could be used for this purpose is not a sufficient triggering factor.

Paragraph 67 of the Guidelines states that if the video surveillance is used to process sensitive data on the basis of Article 9(2)(c) of the GDPR,[4] there should be an "absolute necessity" to safeguard the vital interests of a person. This statement should be nuanced because there could be cases where the processing at hand would need to take place to avoid further harm rather than wait for absolute evidence that the vital interests of the person could be endangered (e.g. suspicion that a sexual encounter captured seems to be developing into a dangerous attack or where someone could be close to committing suicide). This paragraph further refers to the fact that the data controller should not be allowed to use the video surveillance system for any other purpose. This statement should also be nuanced as the processing of personal data is not necessarily based on a single legal ground. The images may have been recorded

[4] Processing necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

initially for legitimate interest grounds or based on consent and subsequently used to protect vital interest of an individual or to comply with a legal duty (e.g. to report an offence).

In addition, CIPL believes that the example in **paragraph 68** where an individual is brought unconscious to the hospital is incomplete given that, even were the data subject is conscious, the appropriate ground for monitoring would likely be Article 9(2)(h) of the GDPR which relates to processing for the purposes of medical diagnosis and healthcare. CIPL suggest including both scenarios in the example.

Finally, CIPL considers that **paragraph 76** of the Guidelines places undue emphasis on explicit consent. Consistent with Article 9(2) of the GDPR, biometric data may also be processed on the basis of a number of other legal bases (see Section II of this Paper under paragraph 76 for more details).

Summary of CIPL Recommendations:

- Amend the example in paragraph 63 to provide that the images of the event will only be a "special category of data" if the controller actually uses the footage to deduce or infer the participant's political opinions.

- Review the statement that there should be an absolute necessity to safeguard the vital interests of the individual to process sensitive data.

- Consider legal bases other than explicit consent for the processing of biometric data for identification purposes.

Data subject rights

CIPL supports the analysis in **paragraph 91** that the information provided by the controller to the data subject requesting access to his/her data can be limited if no data is stored or transferred after the real-time monitoring moment. However, this principle should also apply to requests from data subjects to access "unstructured/non-analysed" CCTV footage based on Article 11 of the GDPR. If the controller only stores CCTV footage without analysing it, the controller is not able to identify the data subject requesting such footage and would need to acquire and process additional information in order to identify the data subject and to respond to the data access request. Furthermore, in the employment context, in large company facilities, the controller may not be in the position to identify the data subject and the data subject may not be able to provide the "additional information" that would enable his/her identification. For example, if an employee asks for "his video footage from camera X on day Y", this would still require additional processing from the controller (use of matching technologies with the company directory that amounts to creating a new processing with a specific purpose). CIPL suggests that paragraphs 95 and 96 be adapted accordingly.

In **paragraph 93**, the Guidelines suggest that the controller should not give access upon request to video footage where other data subjects can be identified while requiring at the same time that data subjects can continue to exercise their legitimate right of access. The Guidelines recommend implementing obfuscating measures in order to fulfil these types of access request. In addition to increasing the technical

burden on video device manufacturers, the requirement of obfuscating measures is too proscriptive and makes inaccurate assumptions about video system capabilities. Technical solutions such as blurring or masking may not be widely available and adapted to the video device specific environment. CIPL recommends that this be balanced against unrealistic exercise of rights of data subjects, in line with Article 25 of the GDPR that requires the data controller to take into account the state of the art as well as the cost of implementation[5] when selecting the appropriate technical and organisational measures to implement data protection principles in an effective manner.

CIPL welcomes the Guidelines' pragmatic approach in **paragraph 94** that in the context of an access request, controllers cannot be obliged to search large amounts of stored material in order to find the personal data in question. However, at **paragraph 105**, CIPL questions the Guidelines' statement that in case of exercise of the right to object, the controller should be obliged to switch off the camera on request, in the absence of special circumstances, given that video recording is most often used to prevent crime. In addition, this position appears impractical, as shoplifters would simply ask their accomplices to "object" to the processing of data via video devices and then benefit from a surveillance-free premises. The need to protect staff and customers as well as to prevent crime must be a "compelling legitimate interest"[6] of the data controller to justify the initial data collection, despite any objections.

With regard to the right of erasure, attention should also be given to video reporting of events, often used for promotional purposes by organisations. Individuals are clearly informed of the recording taking place and offered the right to object before the event. These materials are often compiled at material cost and effort. Erasure of parts of such videos after they have been completed and published would be problematic and disproportionate.

Summary of CIPL Recommendations:

- Add that the information that may be provided to the data subject requesting access to his/her data can be limited in accordance with Article 11 of the GDPR.

- Take into account the state of the art and the cost of implementation in line with Article 25 of the GDPR.

- Recognise that safety and security constitute a compelling interest of the data controller, overriding the data subject's right to object.

Transparency

The Guidelines state in **paragraph 15** that when the purpose of the processing of personal data through video devices is to protect property and other assets, informing data subjects that processing is done for

[5] Paragraph 100 of the Guidelines mentions that "available technology and the cost of implementation" should be taken into account when defining reasonable steps to inform other controllers when the controller has made the video footage public and the data subject has requested that data be erased under Article 17 of the GDPR.
[6] See Article 21(1) of the GDPR.

safety purposes or "for your safety" is not specific enough. Under the GDPR, the transparency obligation requires that meaningful information "using clear and plain language"[7] is provided to the individual. The use of plain language and short expressions enables better understanding by data subjects. In CIPL's opinion, "safety" is a more simple, straightforward and precise wording than the expression "to protect property and other assets" and would be better understood by the average data subject (who will often not read through long notices). CIPL recommends that the Guidelines provide an alternative that would take into account the above and be adapted to the wide range of data subjects that may receive this information.

In **paragraph 112**, the Guidelines' expectations for the "first layer" list of information (details and purposes of processing; identity of the controller; existence of rights of data subjects; greatest impacts of the processing; legitimate interest of the controller; contact details of the DPO; where to find more information) appear unrealistic. Any sign with that much information runs the risk of being unreadable, as the print will be too small. This will run afoul of the obligation to provide information to the data subject in an intelligible manner.[8] Instead, CIPL recommends that controllers focus on communicating the high-level elements of the video recording, simplifying notice elements and directing data subjects clearly to where they may find more information.[9]

Finally, in **paragraph 113**, the Guidelines recommend to include any information that could surprise the data subject such as for instance transmissions to third parties or international transfers. By doing so, the Guidelines ignore that such transmission is not always surprising to data subjects such as in the employment context in multinational companies or in the case of the use of branded security solutions. Similarly, storage instead of live monitoring is also not always surprising to data subjects (e.g. large buildings where it is clear that live monitoring is not a viable option). Therefore, the specific context should also be taken into account when providing information for the sake of more efficient information of the data subject. Article 13(4) of the GDPR also provides clearly that the obligation to provide information does not apply where the data subject already has the information.

Summary of CIPL Recommendations:

- Provide alternative language for video processing done for safety purposes.

- Reduce the list of information required on the first layer of information provided to the data subject to enable intelligibility.

- Take context into account when defining content of information to be provided to the data subject.

[7] See Article 12(1) of the GDPR.
[8] See Article 12(1) of the GDPR.
[9] See CIPL's white paper on "Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR" at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf

6 September 2019

Storage periods and obligations to erase data

Paragraph 119 of the Guidelines suggests strict storage periods with regards to video surveillance and arbitrarily refers to a 72-hour retention period as being the norm, with any longer storage period requiring justification, together with an example in **paragraph 120** mandating deletion of the data after 24 hours. Such paragraph appears predicated on video recordings' only being used for regularly monitored crime prevention and safety purposes, which is overly restrictive. In many instances, such as in relation to IT infrastructure, or fraud, incidents and damages will not immediately be recognised and videos may need to be kept for longer periods, provided of course that video recordings are well protected and access is limited to strict protocols. Retaining the video may, in case of an investigation, be also in the interest of the data subject. CIPL suggests this paragraph be drafted in a more nuanced manner to provide that controllers be able to determine such retention period on a case-by-case basis, taking into account the controller's particular use case, purpose of the processing and risk at stake, as well as the possible mandates of relevant national laws.

Technical and organisational measures

In **paragraph 126**, the Guidelines propose that video surveillance systems should be limited to the functionalities that are necessary to achieve the purpose of the processing whereas those that are not necessary should be deactivated. Such a restriction ignores that functionalities that are not directly necessary for the case at stake can be indirectly necessary to achieve the purpose of the processing by providing more accurate results such as offering highest image definition or better response time. CIPL would therefore suggest to nuance this statement.

II. Comments on facial recognition (paragraphs 72 to 89)

5. 1 General considerations when processing biometric data

While it is clear that the processing of biometric data for the purpose of uniquely identifying a natural person, including through facial recognition, falls under special categories of data and is therefore subject to the provisions of Article 9 of the GDPR, CIPL believes that the Guidelines as they are currently drafted provide for a restrictive interpretation of these provisions that could hinder the beneficial use of facial recognition in several ways. As further explained in this Paper, CIPL recommends that several examples of the Guidelines be reviewed and updated.

Paragraph 72

CIPL wishes to underline that facial recognition technologies bring important benefits for individuals and organisations in many ways (e.g. convenience, authentication, age verification, identity verification for KYC purposes, enhanced security, identification of missing or exploited children). The Guidelines highlight first that facial recognition entails heightened risks for data subjects' rights while agreeing late in the paragraph that "these technologies can be perceived as particularly effective". CIPL would suggest

reframing this paragraph in a more balanced way, referring also to the benefits that facial recognition systems can provide as follows: "The use of biometric data and in particular facial recognition provides important benefits for organisations and individuals, but may, depending on the use case, also entail heightened risks for data subjects' rights".

Paragraph 76

CIPL is concerned with the blanket determination of the Guidelines that the "*use of video surveillance including biometric recognition functionality installed by private entities for their own purposes […] will in most cases require explicit consent*". The qualification of personal data as biometric data subject to Article 9 will require a case-by-case analysis performed by the data controller to verify that the three cumulative criteria of Article 4(14) summarised by the Guidelines in paragraph 75 are met: (1) personal data relating to physical, physiological or behavioural characteristics of a natural person; (2) personal data resulting from a specific technical processing; and (3) personal data used for the purpose of uniquely identifying a natural person.

When one of the three elements of Article 4(14) is missing, the processing of data will not be subject to Article 9 of the GDPR. It will either be subject to the GDPR provisions on the processing of "non-special" categories of personal data that can be performed on the basis of six legal bases[10] (where consent is only one such basis). In the case where the biometric or other data does not relate to an identified or identifiable natural person, it may even be outside of the scope of the GDPR. As the examples below demonstrate, there are several instances where the data is not processed for the purpose of uniquely identifying a person. CIPL believes that the Guidelines should acknowledge that, in some circumstances, a face template may not be personal data at all, if there are no means reasonably likely to be used, or if there are no lawful means, for the controller to identify the individual from the template. This might be the case, for example, if the controller does not have the raw underlying photograph, or the template is only very "basic".

When the qualification of biometric data and application of Article 9 is confirmed, the controller will have to consider the most appropriate legal basis of the processing in the 10 exceptions listed in Article 9(2), (where consent is only one of them) to legitimise the processing. CIPL would recommend that the Guidelines indicate further that, in addition to explicit consent of the data subject, other exceptions under Article 9(2) of the GDPR can be used to permit processing for security purposes even when facial recognition is used for the purpose of uniquely identifying individuals. Depending on the specific circumstances, the following exceptions should also be considered:

- Processing necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment;[11]

[10] See Article 6(1) of the GDPR.
[11] See Article 9(2)(b) of the GDPR. Biometric verification, including facial recognition can be necessary to ensure a safe working environment (e.g. in highly sensitive laboratories, restricted areas such as nuclear plants, clearance of personnel with accredited defense status, etc.).

- Processing necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent;[12]

- Processing necessary for reasons of substantial public interest;[13]

- Processing necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices.[14]

Paragraph 78

The Guidelines provide that (1) the intermediate templates made on the fly in order to be compared to the ones created by the data subjects at the time of the enlistment should be immediately and securely deleted once a match or no-match result has been obtained and (2) the templates created for the enlistment of the individual should not be stored or archived.

CIPL is concerned by both statements for the following reasons:

(1) Intermediate templates created for the "match / no-match" phase consist of a string of numbers with no association to any particular identity or individual. As such, they should not be considered as falling under the category of special categories of data as their purpose is not to uniquely identify a natural person. They do not even amount to processing of personal data. Therefore, CIPL believes that the requirement to have these intermediate templates immediately and securely deleted should be reviewed. This should apply only to the templates enabling the unique identification of an individual in alignment with Article 5(1)(e) of the GDPR.[15] Further, CIPL notes that retaining and comparing these intermediate templates to the biometric template created at the time of enlisting is crucial to ensuring the ongoing efficacy of the identification system as described in further detail below.

(2) Biometric templates created at the time of enlisting. CIPL believes the risks should be better balanced against the benefits of storing these templates. Storing biometric templates enables providers to improve their technology to offer better and more accurate facial recognition services. Storage prohibition of these templates may likely affect users in the long term if providers are unable to enhance their service to provide high-quality face recognition functionalities. This may increase the rate of false positives, causing harm to users that could be

[12] See Article 9(2)(c) of the GDPR. This could for instance enable quicker confirmation of the identity of an individual and facilitate determination of blood group or molecule allergies to provide more expeditious and efficient treatment.
[13] See Article 9(2)(g). This could cover for instance use of facial recognition to access restricted areas.
[14] See Article 9(2)(i). This could cover use of facial recognition technologies for limiting the spread of epidemics in crisis situations.
[15] Data that permits the identification of data subjects cannot be kept longer than is necessary for the purposes for which the personal data are processed.

avoided. Finally, continuous improvement and better accuracy of the technology is increasingly important given the growing concerns over biased and discriminatory facial recognition systems. Further, the resources needed to continuously generate, delete and regenerate biometric templates would be better allocated to research and improvement of the facial recognition systems. Storing and archiving of the biometric templates should of course be done securely in access-controlled environments. The templates should be used only for the purposes consented to by the data subject at the time of enlisting. Users should also be able to easily exercise their rights under the GDPR, including deleting these templates at any time.

Paragraphs 80, 81 & 82

CIPL agrees with the Guidelines that Article 9 of the GDPR should apply only when the technology is used for the purpose of uniquely identifying an individual (i.e. a video footage of an individual could be processed in a manner that generates biometric data, which could then be used for the purpose of uniquely identifying an individual). In addition, CIPL agrees that a distinction must be made between the use of facial recognition technology for the purpose of uniquely identifying an individual and the purpose of classifying an individual based only on physical characteristics. Consistent with the Guidelines' example in paragraph 80, Article 9 would not be applicable in the latter case.

However, CIPL disagrees with the analysis in the Guidelines that considers that merely distinguishing one template from another, or matching two templates, is considered as "uniquely identifying" the underlying data subject and therefore triggers Article 9 requirements. Even singling out to determine that person A has appeared in the same place twice, or appeared in two locations, does not mean that the controller has the purpose of "uniquely identifying a natural person". The test must be whether the purpose of the processing of the templates aims to identify an individual. The same logic applies where the controller distinguishes person A from person B. The simple process of matching or distinguishing two templates does not mean that this processing is done with the purpose of uniquely identifying the individual.

As already explained above, templates do not necessarily enable the identification of the individual. In order to fall under the category of biometric data, a face template needs to meet the additional requirement to be actually used to "allow or confirm unique identification of that natural person". This implies that the controller has other identifying information linked to the face template with which a newly acquired template is matched for unique identification purposes. The person is "uniquely identified" at the point when a template of the individual's physical characteristic is correlated with the pre-existing template connected to identifying information held by the controller. In the absence of this other template and information, the individual cannot be uniquely identified from the newly acquired template. Consequently, processing a face template where there is no such cocorrrelatable data cannot fall under the definition of biometric data under Article 4(14) of the GDPR or even be considered as personal data. Thus, and consistent with paragraphs 79 and 80 of the Guidelines, such a face template that is used only to detect matching faces, is not used for the "purpose of uniquely identifying a person".

There are numerous practical and innocuous examples where controllers may match two biometric templates without any intention and attempt to uniquely identify the data subject. These examples include statistical counting such as for instance the counting of how many people enter their premises and to ensure they do not count the same person twice, queue measurement, calculation of how long it takes to move from the start to the end of a queue. In these examples, the controller simply determines that two face templates are the same (and others are different), with no interest in identifying who is behind each template. Consequently, Article 9 does not apply to these instances.

CIPL wishes to clarify that in general, it is important to differentiate between face characterisation, cases of unique persistent identifier and actual face recognition:

- **Face characterisation** does not involve or allow for the unique identification of a person. Face characterisation may be used for in-store digital sign serving gender-specific advertising (for example men's clothing to a man) or for tracking in-store customer behaviour patterns (for example, pausing in a particular area, or displaying excitement in another) without any purpose to process information by which that individual or individuals could be uniquely identified. (See also example in paragraph 80 of the Guidelines.) Face characterisation may not meet the definition of personal data.

- **Unique persistent identifier** may trigger identifiability of the individual only if it is tied to other unique identifying information. Unique persistent identification would entail that, for a given but limited period, intermediate templates are retained and processed in order to understand if the same person is in a set of photos, or wandering about different aisles in the same store (without being able to identify who that person is in any persistent fashion for example on another day). Face recognition would only apply when those intermediate templates are actually tied to other identifiers and used for the purpose of uniquely identifying the individual.

- **Face recognition must** meet the three requirements of Article 4(14). In particular the processing must be performed by the controller for the specific purpose of uniquely identifying a natural person. The mere fact that the data enables an identification is therefore not sufficient to trigger the application of Article 9 of the GDPR.

Such distinction should be better reflected in paragraph 81 and in the example in paragraph 82. The Guidelines should be more precise, in particular in the description of the possible different cases involved. They should confirm that advertising customisation based on features such as gender or age that do not intend to and actually do not involve the unique identification of a person are out of the scope of the GDPR. Article 9 should apply only if actual biometric templates linked to unique identifying information are built and stored. It should not apply in case of intermediate temporary templates that do not result in the unique identification of a person. CIPL recommends that the example is revised to better capture the possible nuances.

6 September 2019

Paragraphs 83 & 84

For the same reason, CIPL disagrees with the Guidelines' blanket dismissal in paragraph 83 of creating biometric templates "on the fly", without a lawful basis under Article 9. The term *biometric template* needs to be accurately and precisely defined. The fact that a system is capturing on the fly the faces of people passing by does not mean that it is automatically creating biometric templates. There should be a clear distinction between biometric templates created at the time of enlisting with the purpose of uniquely identifying individual and intermediate templates created for the "match / no-match" phase depending on whether they ultimately match or no-match. Again, in this instance, the controller, who seeks to identify person A for whom it retains a biometric face template connected to identifying information, is neither able nor seeking to uniquely identify every other person who steps in front of the camera just by capturing their faces through intermediate templates. The language of Article 4(14) makes it clear that the technical processing must allow or confirm the identification of "that natural person". Where there is no match, the processing does not allow or confirm the identification ("uniquely identifying") of that natural person and is not biometric data subject to explicit consent[16] under Article 9.

On this basis, CIPL recommends that the examples of the Guidelines in paragraph 84 be updated as follows:

- The first example provides that hotel guests that have not given explicit consent to the creation of their biometric template, and to the correspondent use of facial recognition, would still be required to provide consent in order to be monitored by the system and enable proper VIP identification. However, as the system is only creating intermediate templates that will result in no match for all non-VIP guests, it does not trigger (and does not intend to trigger) unique individual identification and therefore does not fall under Article 9.

- The second example provides that in order for biometric templates of non-consenting spectators not to be created by the system, there should be a separate entrance. Again this statement is incorrect as the system will not create biometric templates but only intermediary templates of non-consenting spectators for no-match purposes and that will not result in identification. There should therefore be no requirement to provide for separate entrances.

Paragraph 85

The Guidelines should not include a blanket prohibition on access to services being conditional on biometric processing and require that the data controller offer an alternative solution that does not involve biometric processing:

- The test that must be passed is whether the processing is proportionate (e.g. to avoid fraud or impersonation, access to a bank account for persons who are illiterate, access to an airport

[16] In addition, the requirement to obtain valid consent from all and any "visitor or passer-by" would be quite difficult to manage from an operational perspective, if not impossible.

security) or whether there is a legal obligation that must be complied with (e.g. banks, age verification to access certain contents or services or premises, etc.).

- Under Article 7(4) of the GDPR defining the conditions for valid consent, mandating biometric processing to access a service is one of the factors in determining whether consent is freely given. In accordance with the EDPB guidelines on consent,[17] this is a presumption and not a prohibition. The EDPB should recognise that biometric processing may be inherent to some services, which simply cannot be provided without it (as it would deprive the service of its central value).

- Similarly, having to provide alternative solutions to biometric processing may undermine the whole purpose of the processing. When facial recognition is used for security, authentication and identification purposes (as described in the second example of paragraph 77), requiring the controller to always offer an alternative way to access the building such as through badges or keys would substantially lower the level of security of the building and even put in question the relevance of investing in facial recognition technology for security purposes. This is also particularly problematic in the financial sector using video ID verification products for KYC and anti-money laundering (AML) purposes. The facial recognition involved in this context is consent-based, but the underlying purpose of the processing is to comply with KYC legal obligations which is currently achieved by collecting IDs manually. The global trend is to move towards replacing this manual verification process with automated video ID verification. Companies should not be forced to create additional manual processes when video ID verification has been chosen by the controller as the means to verify their customers for KYC/AML purposes.

Summary of CIPL Recommendations

- Recognise that processing of personal data through facial recognition technologies may be based on several legal bases and not based on only the explicit consent of the data subject.

- Acknowledge that intermediate templates created for matching purposes do not amount to special categories of data.

- Acknowledge that using biometric templates to improve the technology will reduce the risk of harm to individuals.

- Differentiate between face characterisation, unique persistent identifier and actual face recognition.

- Update the examples in paragraphs 82 and 84 in line with CIPL's remarks.

[17] Article 29 Working Party Guidelines on consent under Regulation 2016/679 adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030

- Recognise that biometric—including facial recognition—processing may be inherent to some services.

- Acknowledge that the data controller does not have to offer an alternative solution to biometric processing and update example in paragraph 77 accordingly.

5. 2 Suggested measures to minimise the risks when processing biometric data

Paragraph 89

CIPL considers that the Guidelines currently go too far in suggesting that controllers must always delete the raw data. Rather, the Guidelines should provide that the raw data should be deleted where the controller no longer has a lawful basis to continue processing it in line with Article (5)(e) of the GDPR.

More generally, CIPL urges against the prescriptive approach of the Guidelines and the lack of inclusion of the risk-based approach. While CIPL acknowledges the heightened risk for data subjects of facial recognition technologies, there are instances where the risk to the rights and freedoms to individuals are low—in particular when the technology does not enable uniquely identifying an individual.

Finally while CIPL welcomes the inclusion of a section of the Guidelines on technical organisational measures, we note that it only deals with video surveillance systems and does not include examples that would be relevant in the context of facial recognition technologies. In order to assist organisations in implementing "accountable facial recognition practices", CIPL recommends that the Final Guidelines include examples of accountable practices[18] when developing or using facial recognition technologies.

Summary of CIPL Recommendations

- Provide that the raw data should be deleted where the controller no longer has a lawful basis to continue processing it in line with Article (5)(e) of the GDPR.

- Further take into account the risk-based approach of the GDPR.

- Include examples of accountable practices relating to the facial recognition technologies.

Conclusion

CIPL is grateful for the opportunity to comment on the EDPB's Draft Guidelines 3/2019 on processing of personal data through video devices. If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, Nathalie Laneret, nlaneret@huntonAK.com or Sam Grogan, sgrogan@huntonAK.com.

[18] This could include for instance guidance on the potential sources of risks, threats scenarios and mitigation measures to be included in a DPIA.