Position Paper

Bitkom views on the EDPB Guidelines 3/2019 on processing of personal data through video devices

09/09/2019

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of Trust & Security
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

1. Introduction

Bitkom welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft Guidelines on processing of personal data through video devices. We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice and reduce legal uncertainty. Especially in the field of video surveillance (and other image-related data processing) there is still a lot of uncertainty. In our opinion, the Guidelines should aim at providing practical Guidance and to strike a balance between the interests concerned. That includes, on the one hand, not overly restricting the use of data processing through video devices but on the other hand clarifying which uses are not considered appropriate. Both factors are important to build trust in digital technologies, further innovation and protect the data subject´s rights.

We therefore appreciate that the EDPB published the draft Guidelines and would like to highlight the following aspects of the draft Guidelines before giving detailed comments below:

- The Guidelines should be more specific in their focus as it is not yet clear which elaborations should only be linked to "video surveillance" and which to "processing of personal data through video devices". We suggest limiting the scope of these first Guidelines to only video surveillance and giving guidance on all other cases of processing

through video devices in another Guideline.

- The Guidelines should then strike a balance between all interests concerned when video surveillance or processing through video devices is deployed.
- With regard to the scope of the GDPR in general, it is important to reassess the scope of the household exemption.
- Clarifications about relying on legitimate interests and practicality with regard to the information obligations are still needed in the Guidelines.
- The requirements for special categories of data should include the relevant GDPR definitions of personal data and reassess the situations where data subjects will be uniquely identified.

2. General comments

Bitkom would like to provide some general comments on the Guidelines, as the scope seems to not be clear enough to provide practical guidance. Largely, the guidelines focus clearly on “video surveillance”. Accordingly, the well-known aspects - ultima ratio, storage duration and limitation, information obligations, distinction between "live monitoring" and "recording", camera angle, etc. - are also dealt with. But the Guidelines draw on aspects that are usually not covered when speaking of “video surveillance”. While para 7 provides quite a clear definition in order to define the “scope of application”, the very title of the document is “processing through video devices” which goes considerably further than mere surveillance. This is repeated in para 6.

Further, the provided examples lead to confusion. In the context of the household exemption, the first two examples lie completely outside the scope of video surveillance, as the described cases do not even fulfil the conditions for surveillance set out in para 7. Example 3 even does not include a practical solution for the provided situation since it addresses the problem of third party "visitors" but does not offer a practical answer.

Furthermore, the current scope of the Guidelines seems too broad as they even include processing by optical sensors (even vehicle cameras for parking aids etc. are addressed). The practical consequences would therefore cover so many different scenarios, industries

and devices that it seems questionable whether they can all be properly addressed in this one Guideline.

Bitkom therefore suggests limiting the scope of application and initially concentrate only on video surveillance. Following that the EDPB could offer special Guidelines for specific circumstances and including a reference to the fact that the respective industries could draw up Codes of Conduct in accordance with Art. 40 et seq GDPR.

Within this layered framework, a clear distinction could then be made between surveillance cases by public authorities, by companies and by private individuals.

Limiting the scope would also leave room to include another necessary distinction between the different stages of the processing: Data collection (recording with or without storage), further internal processing, further processing with transfer to third parties / publication. Only with such distinction does it appear possible to provide meaningful solutions for the rights of the data subjects. This is because an objection according to Art. 21 would also have to be processed according to the respective individual processing steps. The current version of the Guidelines provides, for example, for a "preliminary objection" against video surveillance. But how should such an objection be implemented in practice? Either one would come to the conclusion that such an objection always misses its mark, since it is technically impossible to guarantee a non-recording without at least making a recording which determines whether there is someone on the recording to be made who does not want to be recorded. Understandably, this does not seem to be the intention of the EDPB as it would completely contradict the purpose of Art. 21. Distinguishing between the different layers of processing could also provide clarity with regard to the user´s objection to the processing: There might be cases where an objection against the recording might be unfounded due to overriding interests of the controller, but a post-recording processing could be successfully objected against. This could also resolve mixtures in the field of surveillance for several purposes; e.g. surveillance in shopping centres for the purpose of preventing theft and guaranteeing security, with simultaneous evaluation of the recordings for the purpose of customer flow analysis, or other purposes not assigned to classical surveillance.

With regard to the right to object it is in any case questionable that the Guidelines give the impression that the data subject can always object successfully even if Article 21 GDPR clearly states that there might be interests of the controller to take into account.

3. Clarity with regard to video surveillance at conferences, public gatherings etc.

There is still considerable uncertainty with regard to video surveillance and the making of video material at conferences and public gatherings. The Guidelines seem to focus on systematic automates monitoring of a specific space to protect individuals life and health or for property protection purposes. However, everyday uses of videographic material includes the filming of conferences and gatherings as well. Often, this is done for marketing purposes or to assess size, structure and movement of groups of people without focussing on specific individuals. We would therefore welcome guidance on such material as well.

4. Household Exemption

In section 2.3. the Guidelines focus on the Household exemption. The narrow approach taken in the Guidelines needs adjustments. Based on the Lindqvist Decision the Guidelines argue in the Example in para 14 that a private holiday video recording would not fall under the household exemption if it were to be shared online with an indefinite number of people. Blocking the exemption would effectively turn the person that made the private video into a controller and that he would have to comply with all the GDPR-requirements. While finding a legal basis might be possible, the “controller” will not be able to fulfil his information requirements, let alone will he be able to implement the necessary technical and organisational measures etc. His function differs from that of the controller the GDPR had in mind. Restricting the household exemption this extensively would effectively mean that private videos depicting other people could no longer be shared online in a GDPR compliant way (exception only with regard to Art. 85 GDPR). The EDPB should also consider the impact such a decision would have on the users of all the video platforms and social networks. The policy debates surrounding the copyright reform have shown a considerable detachment between policy and society, especially younger internet users. To secure the reputation of the GDPR all stakeholders should tread carefully before interpreting the new framework and provisions in a way that impacts thousands of day-to-day processes.

Furthermore Example 2 would not fall under the GDPR at all, as no personal data is recorded but the downhill mountain biker´s. There would therefore be no need for the household exemption. The example should be amended to include the possibility of her recording other people on her way down the trail.

Also, example 3 is too broad. At the moment, the example would include situations where the neighbouring property is inside the frame of the camera even if the angle would only cover a part of the property where no people ever walk by. The same applies for the coverage of public space – if no personal data is processed, the GDPR does not apply at all.

5. Information about video surveillance

5.1. Information to be conveyed

In para 112 the EDPB's describes the information that has to be conveyed on the 'first layer'. Bitkom suggests amending that paragraph to make it more practicable. Any sign with that much information as described in para 112 will be unreadable, as the print will be too small. In our view, controllers should rather focus on communicating the fact of video recording, and where to find more information. Providing details of data subject´s rights would be particularly problematic with regard to the length of the text that would have to be conveyed on the sign.

5.2. Reasonable Expectation of the Data Subject

In para 39, the Guidelines argue that signs informing the subject about the video surveillance have no relevance when determining what a data subject objectively can expect. In our view, the opposite is the case: If the user is informed about the data processing (through a sign or other means) this information shapes his expectation about which processing is taking place. Why else would the GDPR impose broad information obligations on the controller if not to inform the user about what he has to expect. Para 39 should therefore be amended.

Recital 47 explicitly refers to the "reasonable expectations of the data subjects" in the context of the balancing of interests pursuant to Art. 6 (1) lit. f GDPR. It must also be examined whether a data subject can reasonably foresee, at the time the personal data

are collected and in view of the circumstances under which they are collected, that processing for this purpose may take place. Furthermore, the GDPR legislator focuses on whether the data subject "must expect" this in the concrete situation.
If a controller places a sign referring to video surveillance in a specific case, this is one such circumstance, which must therefore be taken into account in a weighing of interests. Because this leads to the fact that the persons concerned in the individual case (e.g. visitors, who enter a company property) can expect that video surveillance takes place.

6. Data subjects rights

Bitkom welcomes that in the context of access requests para 94 includes the clarification that controllers cannot be obliged to search large amounts of stored material in order to find the data subject in question.

In para 95 the Guidelines elaborate on the right to access and include the following example:
If a data subject is requesting a copy of his or her personal data processed through video surveillance at the entrance of a shopping mall with 30 000 visitors per day, the data subject should specify when he or she passed the monitored area within approximately a two hour- timeframe. If the controller still processes the material a copy of the video footage should be provided. If other data subjects can be identified in the same material then that part of the material should be anonymised (for example by blurring the copy or parts thereof) before giving the copy to the data subject that filed the request.

The anonymization proposed here could mean an enormous and disproportionate effort for the controller, given the average time a person spends in a mall, the number of people passed and the wide angles of usual camera feeds. Screening through all this content again would also mean another processing for each and every person visible on the video.

Furthermore, the context between the remarks in para 95 and the example itself remain unclear.

Para 105 again shows the need to differentiate between the stages of processing (see above). Switching the recording off on request seems questionable in circumstances where video recording is used to prevent crime. Apart from the practical implications and difficulties this would also endanger the purpose of the recording. For instance, any shoplifter could then simply ask his accomplice to object to the processing and then benefit from not being recorded in the store at a specific time. The purpose of crime prevention (this includes above all also the protection of staff and other customers) must be considered a "compelling legitimate interest" despite any objections. After the initial recording and collection the data subject may object and this might be subject to another analysis but should be considered as a separate question.

7. Legal basis for processing

Bitkom would welcome if the Guidelines referenced not only Article 6 para 1 lit a GDPR but also other legal bases such as Article 6 para 1 lit f GDPR in its examples (for example in para 50). This would lead to more diversity and an understanding that consent s but one of six different options. Furthermore, cases where the GDPR is not applicable should be clarified at the beginning of the Guidelines as well. F.i. in the second example in paragraph 8 (recordings from high altitude) it would be helpful to clarify that the GDPR will only apply where the data can be related to a specific identifiable person.

7.1. Lawfulness of processing (legitimate interests)

In our view, para 20 (identifying a legitimate interest) should be amended as it deems to overstate the standard required for a legitimate interest and would lead to disproportionate obligations. The Guidelines request that *"A real-life situation of distress needs to be at hand – such as damages or serious incidents in the past – before starting the surveillance. In light of the principle of accountability, controllers would be well advised to document relevant incidents (date, manner, financial loss) and related criminal charges. Those documented incidents can be a strong evidence for the existence of a legitimate interest."*

From a practical point of view the suggested approach seems overly burdensome especially to small businesses. The example would also include homeowners and places obligations on them that they will – in practice – not be able to meet. In suggesting that the controllers need to collect empirical, localised evidence before deploying a standard

CCTV system to prevent crime and help enforcement and prosecution the Guidelines do not include the consideration that video monitoring has been a fact of retail environments and public area monitoring for several decades now and is an important instrument to prevent shoplifting, vandalism, abuse of staff etc. Those recognised concerns of data processing through video devices must be included in the weighing of the interests concerned. The proposed requirement would therefore, in our view, pose a disproportionate and unnecessary burden and endanger important interests not only of the controller but of the people relying on the security that is provided by video surveillance in public places. The controller's efforts would be better placed ensuring the CCTV system itself was implemented in a manner which respects data minimisation.

7.2. Data Minimisation

The data minimisation principle should also be included in the assessment and proposed handling of dash cams in para 34. The Guidelines appear to link the legitimacy of the use of dash cams to a system that is only activated on impact or another trigger ("important to ensure that this camera is not constantly recording traffic, as well as persons who are near a road."). If the Guidelines would emphasise the need for data minimisation and give guidance on how to implement measures such as limited field of vision, short retention periods, security etc., the interests of all parties could be balanced out without compromising the usefulness provided by the dash cams themselves.

7.3. Scope

At para 37, the Guidelines suggests that data subjects should not be monitored at leisure activities and in places such as sitting areas, restaurants, parks, cinemas etc. Unfortunately, this fails to recognise the high instances of crime in many of these areas, particularly petty theft (pickpocketing), vandalism, assaults etc. There is often a very clear legitimate interest in video monitoring in these areas, to protect the safety and security of those who want to use them lawfully. Additionally, the corresponding example does not mirror the elaborations in para 37 as they point out: *"In toilets data subjects expect not to be monitored. Video surveillance for example to prevent accidents is not proportional."* Restrooms would naturally not be considered *"public areas for leisure activities"* and implementing video surveillance to prevent accidents would only work in the same sense a speeding camera would: If the data subject knows the place where it is installed and

therefore adapts his behaviour beforehand. Bitkom therefore suggests amending this paragraph and the corresponding examples.

Bitkom suggests changing the focus of the Guidelines somewhat to provide more guidance on how to configure the monitoring in a compliant manner instead of focusing only on restricting the use of video monitoring as such. Given the prevalence of video recording, this would be a more effective means of protecting privacy and providing guidance to all the controllers that have to comply with the GDPR. In our view, it would be greatly benefit clarity on the use of video devices to have more guidance on the use of technical means such as avoiding combined audio/video recordings unless necessary, and having very short retention periods.

8. Biometric data and other special categories

Bitkom welcomes the clarification set out in para 60 that video is not always considered to be processing of special categories of data. We do, however, suggest including more explanation in this regard and especially clarify example 2. The images of the event will only be special category data if the controller uses the footage to deduce f.i. the participant's political opinions. The fact that it could be used for this purpose is not sufficient. This should also be included in the elaborations in para 83.

8.1. Legal Bases

The example in para 67 should clarify that the appropriate ground for monitoring in such cases would likely be Article 9 para 2 lit h GDPR (processing for the purposes of medical diagnosis, the provision of healthcare etc.).

In our view, para 76 places too much emphasis on explicit consent as a legal basis although several other bases are available and biometric data may be processed for:

- Scientific research purposes or statistical purposes
- To carry out obligations in the field of employment law, e.g. to ensure a safe and secure working environment
- medical diagnosis or the provision of healthcare.

The second example in paragraph 76, for example, regarding access, does not yet to recognise that biometric entry can be necessary to ensure a safe working environment (e.g. in highly sensitive laboratories, schools etc.). In these circumstances, explicit consent could not be obtained, and the effectiveness of the access controls would be entirely undermined by the provision of an alternative entrance route.

8.2. Scope of "uniquely identifying a person"

With regard to para 81 we suggest including clarification and an amendment because in our view the assessment that merely distinguishing one template from another, or matching two templates, is "uniquely identifying" the underlying data subject is too far reaching. The Guidelines suggest that determining that a person has appeared in the same place twice, or appeared in two locations, would mean that the controller has "uniquely identified" this person. However, this determination alone is not enough to uniquely identify a person and the appropriate test must be whether the processing of the templates enables the controller to identify who exactly the person is. The same logic applies where the controller distinguishes person A from person B. The simple process of matching, or distinguishing, two templates is not identifying the individual: While a face template may already in itself be personal data, the additional requirement set out in Article 4 para 14 GDPR ("allow or confirm unique identification of that natural person") implies that the controller has other identifying information linked to a pre-existing template with which a newly acquired template is matched. The person is only then "uniquely identified" when the data (individual's face, fingerprint etc.), is correlated with the pre-existing template connected to identifying information held by the controller. In the absence of other information, the individual cannot be uniquely identified from the newly acquired data. Consequently, processing a face template where there is no such correlatable data, data cannot fall within Article 4 para 14 GDPR. *A fortiori* such a face template only used to detect matching faces, is not used for the "purpose of uniquely identifying a person" as required by Art. 9 either.

This clarification is of crucial importance in practice as there are numerous practical (and innocuous) examples where controllers may match two biometric templates without any attempt to identify the data subject, f.i, if a store owner uses video processing to count how many people enter the premises but ensure they do not count the same person

twice; or in queue measurement. Another example would be the use of such data to calculate how long it takes to move from the start to the end of a queue. In both examples, the controller has no intention of identifying the individual and the use of video processing simply determines that two face templates are the same (or different), with no interest in who is behind each template. Consequently, Article 9 will not apply. For the same reason, para 83 should be amended. Bitkom would welcome if this aspect would be included in the final version throughout section 5 of the Guidelines.

We also suggest including another aspect in the Guidelines. In some circumstances, the biometric template may not be personal data at all: If there is no means reasonably likely to be used, or no lawful means, for the controller to identify the individual from the biometric template. Practical examples might include situations where the controller does not have the raw underlying photograph, or the biometric template is only very 'basic'.

8.3. Storage Period

With regard to data retention Bitkom suggests an amendment in para 89. The Guidelines suggest that controllers must always delete the raw data. However, the raw data should only be deleted where the controller no longer has a lawful basis to continue processing it. This should be reflected for clarification.

8.4. Providing an Alternative to Processing Biometric Data

In our view, para 77 and 85 should be reassessed as well: In para 77 the Guidelines include the following example: *A controller manages access to his building using a facial recognition method. People can only use this way of access if they have given there explicitly informed consent (according to Article 9 para 2 lit a) beforehand. However, in order to ensure that no one who has not previously given his or her consent is captured, the facial recognition method should be triggered by the data subject himself, for instance by pushing a button. To ensure the lawfulness of the processing, the controller must always offer an alternative way to access the building, without biometric processing, such as badges or keys.*

In para 85 the Guideline explicitly require an alternative authentication method that does not include biometric processing.

The example and wording in para 85 seems to propose that consent would only be valid if an alternative access control method is implemented (such as badges or keys). The provision of an alternative, however, could be construed in a way that the biometric access method does not meet the criteria of Article 5 para 1 lit c GDPR (if an alternative can be provided, is the processing of biometric data still necessary?). The rules for consent should not be interpreted in such a way and the interests of the employer should be included in the interpretation of the Guidelines. We therefore suggest amending the example.

9. Consent, Approval & Objection

In para 105 the Guidelines seem to mix consent and the objection when the processing is based on Article 6 para 1 lit f GDPR. In para 104 the *base legitimate interests* is referenced but the enumeration in para 105 refers to "*the approval from the data subject prior to entering the area*". We would propose clarifying that aspect and including more Guidance about the practical implementation of such approval and/or objection.

Para 105 states *"...In practice this means that unless the controller has compelling legitimate grounds, monitoring an area where natural persons could be identified is only lawful if either (1) the controller is able to immediately stop the camera from processing personal data when requested..."* It remains unclear who should be authorized to demand the stop of video surveillance. Data subjects are already granted such rights in the GDPR, such as deletion. In this respect, it is unclear to what extent they should be able to demand the stop of a legitimate video surveillance pursuant to Art. 6 para 1 lit. f GDPR. Similarly, it is not clear why the possibility to stop/interrupt the video surveillance should be a prerequisite for legality. We suggest a clarification in this regard.

10. Storage Periods and Obligations to Erasure

We would also like to provide comments on the issue of storage periods. The EDPB regularly sees only 1-2 days and a maximum of 72 hours as an appropriate storage time. From practical experience, this timeframe does not suffice in certain situations. For instance, companies may need more time to discover material on burglary attempts that were not discovered in due time et. al. especially over holidays/weekends (especially if the alarm is not triggered due to a minor incident). The Guidelines should also include the

fact that the controller – in line with Art. 5 (1) e GDPR – can determine for how long the CCTV data needs to be retained in order to achieve the legitimate purposes it has been collected for. With an appropriate level of protection (encryption, network separation, principle of dual control...) a longer storage period could also provide the necessary data security and data protection while at the same time giving companies the opportunity to retrieve necessary data after an incident.