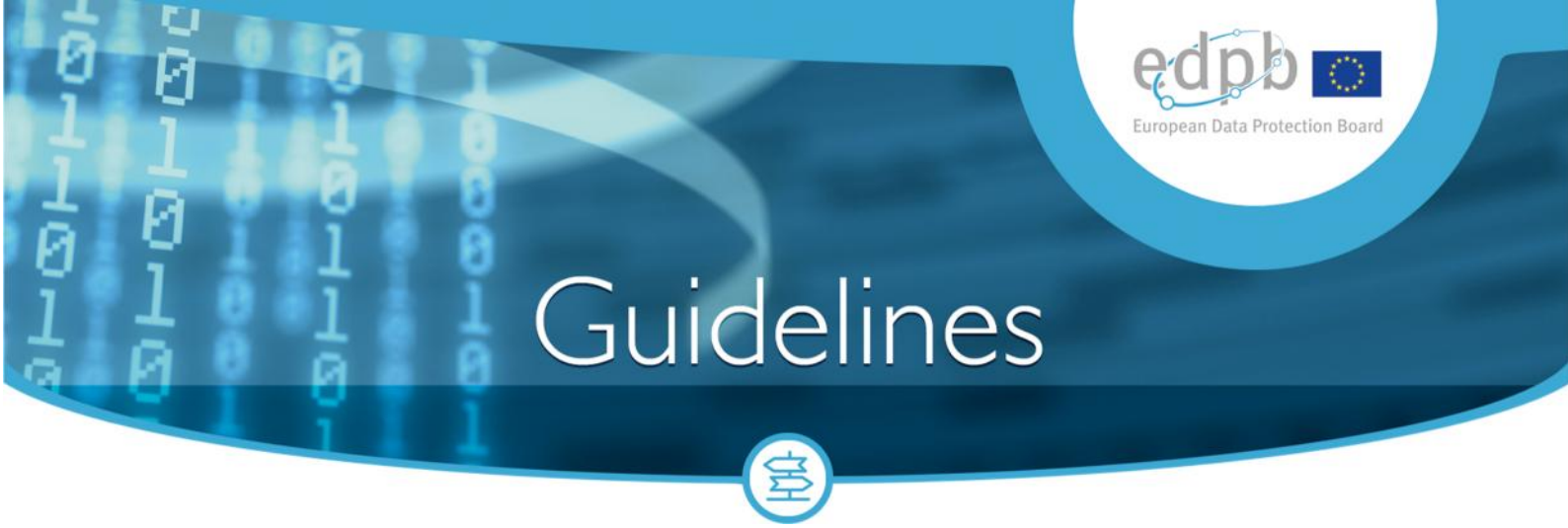


EDPB Plenary meeting, 09-10 July 2019

Guidelines 3/2019 on processing of personal data through video devices

Version for public consultation

Adopted on 10 July 2019

Table of contents

The European Data Protection Board

Having regard to Article 70 (1e) of the Regulation 2016/679/EU 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, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018, revised on 23 November 2018,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. The intensive use of video devices has an impact on citizen's behaviour. Significant implementation of such tools in many spheres of the individuals' life will put an additional pressure on the individual to prevent the detection of what might be perceived as anomalies. De facto, these technologies may limit the possibilities of anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed. Data protection implications are massive.

2. While individuals might be comfortable with video surveillance set up for a certain security purpose for example, guarantees must be taken to avoid any misuse for totally different and – to the data subject – unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.). In addition, many tools are now implemented to exploit the images captured and turn traditional cameras into smart cameras. The amount of data generated by the video, combined with these tools and techniques increase the risks of secondary use (whether related or not to the purpose originally assigned to the system) or even the risks of misuse. The general principles in GDPR (Article 5), should always be carefully considered when dealing with video surveillance.

3. Video surveillance systems in many ways change the way professionals from the private and public sector interact in private or public places for the purpose of enhancing security, obtaining audience analysis, delivering personalized advertising, etc. Video surveillance has become high performing through the growing implementation of intelligent video analysis. These techniques can be more intrusive (e.g. complex biometric technologies) or less intrusive (e.g. simple counting algorithms). Remaining anonymous and preserving one's privacy is in general increasingly difficult. The data protection issues raised in each situation may differ, so will the legal analysis when using one or the other of these technologies.

4. In addition to privacy issues, there are also risks related to possible malfunctions of these devices and the biases they may induce. Researchers report that software used for facial identification, recognition, or analysis performs differently based on the age, gender, and ethnicity of the person it's identifying. Algorithms would perform based on different demographics, thus, bias in facial recognition threatens to reinforce the prejudices of society. That is why, data controllers must also ensure that biometric

data processing deriving from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided.

5. Video surveillance is not by default a necessity when there are other means to achieve the underlying purpose. Otherwise we risk a change in cultural norms leading to the acceptance of lack of privacy as the general outset.

6. These guidelines aim at giving guidance on how to apply the GDPR in relation to processing personal data through video devices. The examples are not exhaustive, the general reasoning can be applied to all potential areas of use.

2 SCOPE OF APPLICATION[1]

2.1 Personal Data

7. Systematic automated monitoring of a specific space by optical or audio-visual means, mostly for property protection purposes, or to protect individual´s life and health, has become a significant phenomenon of our days. This activity brings about collection and retention of pictorial or audio-visual information on all persons entering the monitored space that are identifiable on basis of their looks or other specific elements. Identity of these persons may be established on grounds of these details. It also enables further processing of personal data as to the persons´ presence and behaviour in the given space. The potential risk of misuse of these data grows in relation to the dimension of the monitored space as well as to the number of persons frequenting the space. This fact is reflected by the General Data Protection Regulation in the Article 35 (3) (c) which requires the carrying out of a data protection impact assessment in case of a systematic monitoring of a publicly accessible area on a large scale, as well as in Article 37 (1) (b) which requires processors to designate a data protection officer, if the processing operation by its nature entails regular and systematic monitoring of data subjects.

8. However, the Regulation does not apply to processing of data that has no reference to a person, e.g. if an individual cannot be identified, directly or indirectly.

> Example: The GDPR is not applicable for fake cameras (i.e. any camera that is not functioning as a camera and thereby is not processing any personal data). *However, in some Member States it might be subject to other legislation.*
>
> Example: Recordings from a high altitude only fall under the scope of the GDPR if under the circumstances the data processed can be related to a specific person.
>
> Example: A video camera is integrated in a car for providing parking assistance. If the camera is constructed or adjusted in such a way that it does not collect any information relating to a natural person (such as licence plates or information which could identify passers-by) the GDPR does not apply.

9.

2.2 Application of the Law Enforcement Directive, LED (EU2016/680)

10. Notably processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

---

1 The EDPB notes that where the GDPR so allows, specific requirements in national legislation might apply.

including the safeguarding against and the prevention of threats to public security, falls under the directive EU2016/680.

2.3 Household exemption

11. Pursuant to Article 2 (2) (c), the processing of personal data by a natural person in the course of a purely personal or household activity, which can also include online activity, is out of the scope of the GDPR.[2]

12. This provision – the so-called household exemption – in the context of video surveillance must be narrowly construed. Hence, as considered by the European Court of Justice, the so called "household exemption" must "*be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*".[3] Furthermore, if a video surveillance system, to the extent it involves the constant recording and storage of personal data and covers, "*even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity for the purposes of the second indent of Article 3(2) of Directive 95/46"*[4].

13. What regards video devices operated inside a private person's premises, it may fall under the household exemption. It will depend on several factors, which all have to be considered in order to reach a conclusion. Besides the above mentioned elements identified by ECJ rulings, the user of video surveillance at home needs to look at whether he has some kind of personal relationship with the data subject, whether the scale or frequency of the surveillance suggests some kind of professional activity on his side, and of the surveillance's potential adverse impact on the data subjects. The presence of any single one of the aforementioned elements does not necessarily suggest that the processing is outside the scope of the household exemption, an overall assessment is needed for that determination.

2 See also Recital 18.

3 European Court of Justice, Judgment in Case C-101/01, *Bodil Lindqvist case*, 6th November 2003, para 47.

4 European Court of Justice, Judgment in Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 11 December 2014, para. 33.

Example: A tourist is recording videos both through his mobile phone and through a camcorder to document his holidays. He shows the footage to friends and family but does not make it accessible for an indefinite number of people. This would fall under the household exemption.

Example: A downhill mountainbiker wants to record her descent with an actioncam. She is riding in a remote area and only plans to use the recordings for her personal entertainment at home. This would fall under the household exemption.

Example: Somebody is monitoring and recording his own garden. The property is fenced and only the controller himself and his family are entering the garden on a regular basis. This would fall under the household exemption, provided that the video surveillance does not extend even partially to a public space or neighbouring property.

14.

3 LAWFULNESS OF PROCESSING

15. Before use, the purposes of processing have to be specified in detail (Article 5 (1) (b)). Video surveillance can serve many purposes, e.g. protection of property and other assets, collecting evidence for civil claims.[5] These monitoring purposes should be documented in writing (Article 5 (2)) and need to be specified for every surveillance camera in use. Cameras that are used for the same purpose by a single controller can be documented together, as long as every camera in use has a documented purpose. Furthermore, data subjects must be informed of the purpose(s) of the processing in accordance with Article 13 (*see section 7, Transparency and information obligations*). Video surveillance based on the mere purpose of "safety" or "for your safety" is not sufficiently specific (Article 5 (1) (b)). It is furthermore contrary to the principle that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (see Article 5 (1) (a)).

16. In principle, every legal ground under Article 6 (1) can provide a legal basis for processing video surveillance data. For example, Article 6 (1) (c) applies, where national law stipulates an obligation to video surveillance.[6] However in practice, the provisions most likely to be used are

- Article 6 (1) (f) (legitimate interest).
- Article 6 (1) (e) (necessity to perform a task carried out in the public interest or in the exercise of official authority)

In rather exceptional cases Article 6 (1) (a) (consent) might be used as a legal basis by the controller.

3.1 Legitimate interest, Article 6 (1) (f)

17. The legal assessment of Article 6 (1) (f) should be based on the following criteria in compliance with Recital 47.

5 Rules on collecting evidence for civil claims varies in member states.

6 These guidelines do not analyse or go into details of national law that might differ between member states.

3.1.1 Existence of legitimate interests

18. Video surveillance is lawful if it is necessary in order to meet the purpose of a legitimate interest pursued by a controller or a third party, unless such interests are overridden by the data subject's interests or fundamental rights and freedoms (Article 6 (1) (f)). Legitimate interests pursued by a controller or a third party can be legal,[7] economic or non-material interests.[8] However, the controller should consider that if a the data subject objects to the surveillance in accordance with Article 21 the controller can only proceed with the video surveillance of that data subject if it is a *compelling* legitimate interest which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

19. Given a real and hazardous situation, the purpose to protect property against burglary, theft or vandalism can constitute a legitimate interest for video surveillance.

20. The legitimate interest needs to be of real existence and has to be a present issue (i.e. it must not be fictional or speculative)[9]. 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.

> Example: A shop owner wants to open a new shop and wants to install a video surveillance system. He can show, by presenting statistics, that there is a high expectation of vandalism in the near neighbourhood. Also, experience from neighbouring shops is useful. It is not necessary that a damage to the controller in question must have occurred. It is however not sufficient to present national or general crime statistic without analysing the area in question or the dangers for this specific shop.

21.

22. Imminent danger situations may constitute a legitimate interest, such as shops selling precious goods (e.g. jewellers), or areas that are known to be typical crime scenes for property offences (e. g. petrol stations).

23. The GDPR also clearly states that public authorities cannot rely their processing on the grounds of legitimate interest, as long as they are carrying out their tasks, Article 6 (1) sentence 2.

3.1.2 Necessity of processing

24. Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'), see Article 5 (1) (c). Before installing a video-surveillance system the controller should always critically examine if this measure is firstly suitable to attain the desired goal, and secondly adequate and necessary for its purposes. Video surveillance measures should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means which are less intrusive to the fundamental rights and freedoms of the data subject.

25. Given the situation that a controller wants to prevent property related crimes, instead of installing a video surveillance system the controller could also take alternative security measures such as fencing the property, installing regular patrols of security personnel, using gatekeepers, providing better

7 European Court of Justice, Judgment in Case C-13/16, *Rīgas satiksme case*, 4 may 2017

8 see wp 217, Article 29 Working Party.

9 see wp 217, Article 29 Working Party, p. 24 seq.

lighting, installing security locks, tamper-proof windows and doors or applying anti-graffiti coating or foils to walls. Those measures can be as effective as video surveillance systems against burglary, theft and vandalism.

26. Before operating a camera system, the controller is obliged to assess where and when video surveillance measures are strictly necessary. Usually a surveillance system operating at night-time as well as outside the regular working hours will meet the needs of the controller to prevent any dangers to his property.

27. In general, the necessity to use video surveillance to protect the controllers' premises ends at the property boundaries.[10] However, there are cases where the surveillance of the property is not sufficient for an effective protection. In some individual cases it might be necessary to exceed the video surveillance to the immediate surroundings of the premises. In this context, the controller should consider physical and technical means, for example blocking out or pixelating not relevant areas.

> Example: A bookshop wants to protect its premises against vandalism. In general, cameras should only be filming the premises itself because it is not necessary to watch neighbouring premises or public areas in the surrounding of the bookshop premises for that purpose.

28.

29. Questions concerning the processing's necessity also arise regarding the way evidence is preserved. In some cases it might be necessary to use black box solutions where the footage is automatically deleted after a certain storage period and only accessed in case of an incident. In other situations it might not be necessary to record the video material at all but more appropriate to use real-time monitoring instead. The decision between black box solutions and real-time monitoring should also be based on the purpose pursued. If for example the purpose of video surveillance is the preservation of evidence, real-time methods are usually not suitable. Sometimes real-time monitoring may also be more intrusive than storing and automatically deleting material after a limited timeframe. The data minimisation principle must be regarded in this context (Article 5 (1) (c)). It should also be kept in mind that it might be possible that the controller could use security personnel instead of video surveillance that are able to react and intervene immediately.

3.1.3 Balancing of interests

30. Presuming that video surveillance is necessary to protect the legitimate interests of a controller, a video surveillance system may only be put in operation, if the legitimate interests of the controller or those of a third party (e.g. protection of property or physical integrity) are not overridden by the interests or fundamental rights and freedoms of the data subject. The controller needs to consider 1) to what extent the monitoring affects legitimate interests, fundamental rights, and freedoms of individuals and 2) if this causes violations or negative consequences with regard to the data subject's rights. In fact, balancing the interests is mandatory. Fundamental rights and freedoms on one hand and the controller's legitimate interests on the other hand have to be evaluated and balanced carefully.

10 This might also be subject to national legislation in some member states.

Example: A private parking company has documented reoccurring problems with thefts in the cars parked. The parking area is an open space and can be easily accessed by anyone, but is clearly marked with signs and road blockers surrounding the space. The parking company have a legitimate interest (preventing thefts in the customer's cars) to monitor the area during the time of day that they are experiencing problems. Data subjects are monitored in a limited timeframe, they are not in the area for recreational purposes and it is also in their own interest that thefts are prevented. The interest of the data subjects not to be monitored is in this case overridden by the controller's legitimate interest.

Example: A restaurant decides to install video cameras in the restrooms to control the tidiness of the sanitary facilities. In this case the rights of the data subjects clearly overrides the interest of the controller, therefore cameras can't be installed there.

31.

3.1.3.1 Making case-by-case decisions

32. As the balancing of interests is mandatory according to the regulation, the decision has to be made on a case-by-case basis (see Article 6 (1) (f)). Referencing abstract situations or comparing similar cases to one another is insufficient. The controller has to evaluate the risks of the intrusion of the data subject's rights; here the decisive criterion is the intensity of intervention for the rights and freedoms of the individual.

33. Intensity can inter alia be defined by the type of information that is gathered (information content), the scope (information density, spatial and geographical extent), the number of data subjects concerned, either as a specific number or as a proportion of the relevant population, the situation in question, the actual interests of the group of data subjects, alternative means, as well as by the nature and scope of the data assessment.

34. Important balancing factors can be the size of the area, which is under surveillance and the amount of data subjects under surveillance. The use of video surveillance in a remote area (e. g. to watch wildlife or to protect critical infrastructure such as a privately owned radio antenna) has to be assessed differently than video surveillance in a pedestrian zone or a shopping mall.

Example: If a dash cam is installed (e. g. for the purpose of collecting evidence in case of an accident), it is important to ensure that this camera is not constantly recording traffic, as well as persons who are near a road. Otherwise the interest in having video recordings as evidence in the more theoretical case of a road accident cannot justify this serious interference with data subject's rights.[11]

11 .

3.1.3.2 Data subjects' reasonable expectations

35. According to Recital 47, the existence of a legitimate interest needs careful assessment. Here the reasonable expectations of the data subject at the time and in the context of the processing of its personal data have to be included. Concerning systematic monitoring, the relationship between data subject and controller may vary significantly and may affect what reasonable expectations the data subject might have. The interpretation of the concept of reasonable expectations should not only be

11 Even if under some circumstances it might theoretically be possible to identify a legal basis for parts of such surveillance, the controller will still have to comply with the general principles (Art. 5 GDPR) and the transparency obligations to properly inform the data subject (Art. 13 GDPR).

based on the subjective expectations in question. Rather, the decisive criterion has to be if an objective third party could reasonably expect and conclude to be subject to monitoring in this specific situation.

36. For instance, an employee in his/her workplace is in most cases not likely expecting to be monitored by his or her employer.[12] Furthermore, monitoring is not to be expected in one's private garden, in living areas, or in examination and treatment rooms. In the same vein, it is not reasonable to expect monitoring in sanitary or sauna facilities – monitoring such areas is an intense intrusion into the rights of the data subject. The reasonable expectations of data subjects are that no video surveillance will take place in those areas. On the other hand, the customer of a bank might expect that he/she is monitored inside the bank or by the ATM.

37. Data subjects can also expect to be free of monitoring within public areas especially if those public areas are typically used for recovery, regeneration, and leisure activities as well as in places where individuals stay and/or communicate, such as sitting areas, tables in restaurants, parks, cinemas and fitness facilities. Here the legitimate interests or rights and freedoms of the data subject will often override the controller's legitimate interests.

> Example: In toilets data subjects expect not to be monitored. Video surveillance for example to prevent accidents is not proportional.

38.

39. Signs informing the subject about the video surveillance have no relevance when determining what a data subject objectively can expect.

3.2 Necessity to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, Article 6 (1) (e)

40. Personal data could be processed through video surveillance under Article 6 (1) (e) if it is necessary to perform a task carried out in the public interest or in in the exercise of official authority.[13] It may be that the exercise of official authority does not allow for such processing, but other legislative bases such as "health and safety" for the protection of employees, visitors and employees may provide limited scope for processing, while still having regard for GDPR obligations and data subject rights.

41. Member States may maintain or introduce specific national legislation for video surveillance to adapt the application of the rules of the GDPR by determining more precisely specific requirements for processing as long as it is in accordance with the principles laid down by the GDPR (e.g. storage limitation, proportionality).

12 See also: Article 29 Working Party, Opinion 2/2017 on data processing at work, WP249, adopted on 8 June 2017.

13 The basis for the processing referred shall be laid down by Union law or Member State law» and «shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6 (3)).

3.3 Consent, Article 6 (1) (a)

42. Consent has to be freely given, specific, informed and unambiguous as described in the guidelines on consent.[14]

43. Regarding systematic monitoring, the data subject's consent can only serve as a legal basis in accordance with Article 7 (see Recital 43) in exceptional cases. It is in the surveillance's nature that this technology monitors an unknown number of people at once. The controller will hardly be able to prove that the data subject has given consent prior to processing of its personal data (Article 7 (1)). Assumed that the data subject withdraws its consent it will be difficult for the controller to prove that personal data is no longer processed (Article 7 (3)).

> Example: Athletes may request monitoring during individual exercises in order to analyse their techniques and performance. On the other hand, where a sports club takes the initiative to monitor a whole team for the same purpose, consent will often not be valid, as the individual athletes may feel pressured into giving consent so that their refusal of consent does not adversely affect teammates.

44.

45. If the controller wishes to rely on consent it is his duty to make sure that every data subject who enters the area which is under video surveillance has given her or his consent. This consent has to meet the conditions of Article 7. Entering a marked monitored area (e.g. people are invited to go through a specific hallway or gate to enter a monitored area), does not constitute a statement or a clear affirmative action needed for consent, unless it meets the criteria of Article 4 and 7 as described in the guidelines on consent.[15]

46. Given the imbalance of power between employers and employees, in most cases employers should not rely on consent when processing personal data, as it is unlikely to be freely given. The guidelines on consent should be taken into consideration in this context.

47. Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context (see Article 88).

4 DISCLOSURE OF VIDEO FOOTAGE TO THIRD PARTIES

48. In principle, the general regulations of the GDPR apply to the disclosure of video recordings to third parties.

4.1 Disclosure of video footage to third parties in general

49. Disclosure is defined in Article 4 (2) as transmission (e.g. individual communication), dissemination (e.g. publishing online) or otherwise making available. Third parties are defined in Article 4 (10). Where disclosure is made to third countries or international organisations, the special provisions of Article 44 et seq. also apply.

---

14 In addition, the Article 29 Working Party (Art. 29 WP) adopted „Guidelines on consent under Regulation 2016/679" (WP 259 rev. 01) which should be taken in account.

15 In addition, the Article 29 Working Party (Art. 29 WP) adopted „Guidelines on consent under Regulation 2016/679" (WP 259) which should be taken in account.

50. Any disclosure of personal data is a separate kind of processing of personal data for which the controller needs to have a legal basis in Article 6.

> Example: A controller who wishes to upload a recording to the Internet needs to rely on a legal basis for that processing, for instance by obtaining consent from the data subject according to Article 6 (1) (a).

51.

52. The transmission of video footage to third parties for the purpose other than that for which the data has been collected is possible under the rules of Article 6 (4).

> Example: Video surveillance of a barrier (at a parking lot) is installed for the purpose of resolving damages. A damage occurs and the recording is transferred to a lawyer to pursue a case. In this case the purpose for recording is the same as the one for transferring.
>
> Example: Video surveillance of a barrier (at a parking lot) is installed for the purpose of resolving damages. The recording is published online for pure amusement reasons. In this case the purpose has changed and is not compatible with the initial purpose. It would furthermore be problematic to identify a legal basis for that processing (publishing).

53.

54. A third party recipient will have to make its own legal analysis, in particular identifying its legal basis under Article 6 for his processing (e.g. receiving the material).

4.2 Disclosure of video footage to law enforcement agencies

55. The disclosure of video recordings to law enforcement agencies is also an independent process, which requires a separate justification for the controller.

56. According to Article 6 (1) (c), processing is legal if it is necessary for compliance with a legal obligation to which the controller is subject. Although the applicable police law is an affair under the sole control of the member states, there are most likely general rules that regulate the transfer of evidence to law enforcement agencies in every member state. The processing of the controller handing over the data is regulated by the GDPR. If national legislation requires the controller to cooperate with law enforcement (e. g. investigation), the legal basis for handing over the data is legal obligation under Article 6 (1) (c).

57. The purpose limitation in Article 6 (4) is then often unproblematic, since the disclosure explicitly goes back to member state law. A consideration of the special requirements for a change of purpose in the sense of lit. a - e is therefore not necessary.

> Example: A shop owner record footage at its entrance. It records a person stealing another person's wallet. The police asks the controller to hand over the material in order to assist in their investigation. In that case the shop owner would use the legal basis under Article 6 (1) (c) (legal obligation) read in conjunction with the relevant national law for the transfer processing.
>
> Example: A camera is installed in a shop for security reasons. The shop owner believes he has recorded something suspicious in his footage and decides to send the material to the police (without any indication that there is an ongoing investigation of some kind). In this case the shop owner has to assess whether the conditions under, in most cases, Article 6 (1) (f) are met.

58.

59. The processing of the personal data by the law enforcement agencies themselves does not follow the GDPR (see Article 2 (2) (d)), but follows instead the Law Enforcement Directive (EU2016/680).

5 PROCESSING OF SPECIAL CATEGORIES OF DATA

60. Video surveillance systems usually collect massive amounts of personal data which may reveal data of a highly personal nature and even special categories of data. Indeed, apparently non-significant data originally collected through video can be used to infer other information to achieve a different purpose (e.g. to map an individual's habits). However, video surveillance is not always considered to be processing of special categories of personal data.

> Example: Video footage showing a data subject wearing glasses or using a wheel chair are not per se considered to be special categories of personal data.

61.

62. However, if the video footage is processed to deduce special categories of data Article 9 applies.

> Example: Political opinions could for example be deduced from images showing identifiable data subjects taking part in an event, engaging in a strike, etc. This would fall under Article 9.
>
> Example: A hospital installing a video camera in order to monitor a patient's health condition would be considered as processing of special categories of personal data (Article 9).

63.

64. In general, as a principle, whenever installing a video surveillance system careful consideration should be given to the data minimization principle. Hence, even in cases where Article 9 (1) does not apply, the data controller should always try to minimize the risk of capturing footage revealing other sensitive data (beyond Article 9), regardless of the aim.

> Example: Video surveillance capturing a church does not per se fall under Article 9. However, the controller has to conduct an especially careful assessment under Article 6 (1) (f) taken into account the nature of the data as well as the risk of capturing other sensitive data (beyond Article 9) when assessing the interests of the data subject.

65.

66. If a video surveillance system is used in order to process special categories of data, the data controller must identify both an exception for processing special categories of data under Article 9 (i.e. an exemption from the general rule that one should not process special categories of data) and a legal basis under Article 6.

67. For instance, Article 9 (2) (c) (processing is 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) could – in theory and exceptionally – be used, but the data controller would have to justify it as an absolute necessity to safeguard the vital interests of a person and prove that this person "*is physically or legally incapable of giving his consent*". In addition, the data controller won't be allowed to use the system for any other reason.

> Example: A hospital is monitoring a patient for medical reasons. The data subject was brought by ambulance unconscious to the hospital. In this case Article 9 (2) (c) could apply.

68.

69. It is important to note here that every exemption listed in Article 9 is not likely to be usable to justify processing of special categories of data through video surveillance. More specifically, data controllers processing those data in the context of video surveillance cannot rely on Article 9 (2) (e), which allows processing that relates to personal data that are manifestly made public by the data subject. The mere fact of entering into the range of the camera does not imply that the data subject intends to make public special categories of data relating to him or her.

70. Furthermore, processing of special categories of data requires a heightened and continued vigilance to certain obligations; for example high level of security and data protection impact assessment where necessary.

> Example: An employer must not use video surveillance recordings showing a demonstration in order to identify strikers.

71.

5.1 General considerations when processing biometric data

72. The use of biometric data and in particular facial recognition entail heightened risks for data subjects' rights. It is crucial that recourse to such technologies takes place with due respect to the principles of lawfulness, necessity, proportionality and data minimisation as set forth in the GDPR. Whereas the use of these technologies can be perceived as particularly effective, controllers should first of all assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing.

73. To qualify as biometric data as defined in the GDPR, processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply a measurement of this characteristics. Since biometric data is the result of such measurements, the GDPR states in its Article 4.14 that it is "*resulting from specific technical processing relating to the physical, physiological or behavioural characteristics".* The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual. [16]

74. In order for it to be considered as processing of special categories of personal data (Article 9) it requires that biometric data is processed "for the purpose of uniquely identifying a natural person".

75. To sum up, in light of Article 4.14 and 9, three criteria must be considered:

- **Nature of data :** data relating to physical, physiological or behavioural characteristics of a natural person,
- **Means and way of processing** : data "resulting from a specific technical processing",
- **Purpose of processing:** data must be used for the purpose to uniquely identifying a natural person.

76. The use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require

16 Recital 51 supports this analysis, stating that "*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*".

explicit consent of all data subjects (Article 9 (2) (a)), however another suitable exception in Article 9 could also be applicable.

> Example: To improve its service a private company replaces passenger identification check points within an airport (luggage drop-off, boarding) with video surveillance systems that use facial recognition techniques to verify the identity of the passengers that have chosen to consent to such a procedure. Since the processing falls under Article 9, the passengers, who will have previously given their explicit and informed consent, will have to enlist themselves at for example an automatic terminal in order to create and register their facial template associated with their boarding pass and identity. The check points with facial recognition need to be clearly separated, e. g. the system must be installed within a gantry so that the biometric templates of non-consenting person will not be captured. Only the passengers, who will have previously given their consent and proceeded with their enrolment, will use the gantry equipped with the biometric system.
>
> 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 (2) (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.

77.

78. In this type of cases, where biometric templates are generated, controllers shall ensure that once a match or no-match result has been obtained, all the intermediate templates made on the fly (with the explicit and informed consent of the data subject) in order to be compared to the ones created by the data subjects at the time of the enlistment, are immediately and securely deleted. The templates created for the enlistment should only be retained for the realisation of the purpose of the processing and should not be stored or archived.

79. However, when the purpose of the processing is for example to distinguish one category of people from another but not to uniquely identify anyone the processing does not fall under Article 9.

> Example: A shop owner would like to customize its advertisement based on gender and age characteristics of the customer captured by a video surveillance system. If that system does not generate biometric templates in order to uniquely identify persons but instead just detects those physical characteristics and consequently only classifies the person, then the processing would not fall under Article 9.

80.

81. However, Article 9 applies if the controller stores biometric data (most commonly through templates that are created by the extraction of key features from the raw form of biometric data (e.g. facial measurements from an image)) in order to uniquely identify a person. If a controller wishes to detect a data subject re-entering the area or entering another area (for example in order to project continued customized advertisement), the purpose would then be to uniquely identify a natural person, meaning that the operation would from the start fall under Article 9. This could be the case if a controller stores generated templates to provide further tailored advertisement on several billboards throughout different locations inside the shop. Since the system is using physical characteristics to detect specific individuals coming back in the range of the camera (like the visitors of a shopping mall) and tracking

them, it would constitute a biometric identification method because it is aimed at recognition through the use of specific technical processing.

> Example: A shop owner has installed facial recognition system inside his shop in order to customize its advertisement towards individuals. The data controller has to obtain the explicit and informed consent of all data subjects before using this biometric system and delivering tailored advertisement. The system would be unlawful if it captures visitors or passer-by who have not consented to the creation of their biometric template, even if their template is deleted within the shortest possible period. Indeed, these temporary templates constitute biometric data processed in order to uniquely identify a person who may not want to receive targeted advertisement.

82.

83. The EDPB observes that some biometric systems are installed in uncontrolled environment[17], which means that the system involves capturing on the fly the faces of any individual passing in the range of the camera, including persons who have not consented to the biometric device, and thereby creating biometric templates. These templates are compared to the ones created of data subjects having given their prior consent during an enlistment process (i.e. a biometric devise user) in order for the data controller to recognise whether the person is a biometric device user or not. In this case, the system is often designed to discriminate the individuals it wants to recognize from a database from those who are not enlisted. Since the purpose is to uniquely identify natural persons, an exception under Article 9 (2) GDPR is still needed for anyone captured by the camera.

> Example: A hotel uses video surveillance to automatically alert the hotel manager that a VIP has arrived when the face of the guest is recognized. These VIPs have priory given their explicit consent to the use of facial recognition before being recorded in a database established for that purpose. These processing systems of biometric data would be unlawful unless all other guests monitored (in order to identify the VIPs) have consented to the processing according to Article 9 (2) (a) GDPR.
>
> Example: A controller installs a video surveillance system with facial recognition at the entrance of the concert hall he manages. The controller must set up clearly separated entrances; one with a biometric system and one without (where you instead for example scan a ticket). The entrances equipped with biometric devices, must be installed and made accessible in a way that prevents the system from capturing biometric templates of non-consenting spectators.

84.

85. Finally, when the consent is required by Article 9 GDPR, the data controller shall not condition the access to its services to the acceptance of the biometric processing. In other words and notably when the biometric processing is used for authentication purpose, the data controller must offer an alternative solution that does not involve biometric processing – without restraints or additional cost for the data subject. This alternative solution is also needed for persons who do not meet the constraints of the biometric device (enrolment or reading of the biometric data impossible, disability situation making it difficult to use, etc.) and in anticipation of unavailability of the biometric device

17 It means that the biometric device is located in a space open to the public and is able to work on anyone passing by, as opposed to the biometric systems in controlled environments that can be used only by consenting person's participation.

(such as a malfunction of the device), a "back-up solution" must be implemented to ensure continuity of the proposed service, limited however to exceptional use.

5.2 Suggested measures to minimize the risks when processing biometric data

86. In compliance with the data minimization principle, data controllers must ensure that data extracted from a digital image to build a template will not be excessive and will only contain the information required for the specified purpose, thereby avoiding any possible further processing. Measures should be put in place to guarantee that templates cannot be transferred across biometric systems.

87. Identification and authentication/verification are likely to require the storage of the template for use in a later comparison. The data controller must consider the most appropriate location for storage of the data. In an environment under control (delimited hallways or checkpoints), templates shall be stored on an individual device kept by the user and under his or her sole control (in a smartphone or the id card) or - when needed for specific purposes and in presence of objective needs - stored in a centralized database in an encrypted form with a key/secret solely in the hands of the person to prevent unauthorised access to the template or storage location. If the data controller cannot avoid having access to the templates, he must take appropriate steps to ensure the security of the data stored. This may include encrypting the template using a cryptographic algorithm.

88. In any case, the controller shall take all necessary precautions to preserve the availability, integrity and confidentiality of the data processed. To this end, the controller shall notably take the following measures: compartmentalize data during transmission and storage, store biometric templates and raw data or identity data on distinct databases, encrypt biometric data, notably biometric templates, and define a policy for encryption and key management, integrate an organisational and technical measure for fraud detection, associate an integrity code with the data (for example signature or hash) and prohibit any external access to the biometric data.

89. Besides, data controllers shall proceed to the deletion of raw data (face images, speech signals, the gait, etc.) and ensure the effectiveness of this deletion. Indeed, insofar as biometric templates derives from such data, one can consider that the constitution of databases could represent an equal if not even bigger threat (because it may not always be easy to read a biometric template without the knowledge on how it was programmed, whereas raw data will be the building block of any template). In case the data controller would need to keep such data, noise-additive method (such as watermarking) must be explored, which would render the creation of the template ineffective. The controller must also delete biometric data and templates in the event of unauthorized access to the read-comparison terminal or storage server and delete any data not useful for further processing at the end of the biometric device's life.

6 RIGHTS OF THE DATA SUBJECT

90. Due to the character of data processing when using video surveillance some data subject’s rights under GDPR serves further clarification. This chapter is however not exhaustive, all rights under the GDPR applies to processing of personal data through video surveillance.

6.1 Right to access

91. A data subject has the right to obtain confirmation from the controller as to whether or not their personal data are being processed. For video surveillance this means that if no data is stored or transferred in any way then once the real-time monitoring moment has passed the controller could only give the information that no personal data is any longer being processed (besides the general

information obligations under Article 13, see *section 7 – Transparency and information obligations*). If however data is still being processed at the time of the request (i.e. if the data is stored or continuously processed in any other way), the data subject should receive access and information in accordance with Article 15.

92. There are however, a number of limitations that may in some cases apply in relation to the right to access.

- Article 15 (4) GDPR, adversely affect the rights of others

93. Given that, any number of data subjects may be recorded in the same sequence of video surveillance a screening would then cause additional processing of personal data of other data subjects. If the data subject wishes to receive a copy of the material (article 15 (3)), this could adversely affect the rights and freedoms of other data subject in the material. To prevent that effect the controller should therefore take into consideration that due to the intrusive nature of the video footage the controller should not in some cases hand out video footage where other data subjects can be identified. The protection of the rights of third parties should however not be used as an excuse to prevent legitimate claims of access by individuals, the controller should instead implement technical measures to fulfil the access request (for example, image-editing such as masking or scrambling).

- Article 11 (2) GDPR, controller is unable to identify the data subject

94. If the video footage is not searchable for personal data, (i.e. the controller would likely have to go through a large amount of stored material in order to find the data subject in question) the controller may be unable to identify the data subject.

95. For these reasons the data subject should (besides identifying themselves including with identification document or in person) in its request to the controller, specify when – within a reasonable timeframe in proportion to the amount of data subjects recorded – he or she entered the monitored area. The controller should notify the data subject beforehand on what information is needed in order for the controller to comply with the request. If the controller is able to demonstrate that it is not in a position to identify the data subject, the controller must inform the data subject accordingly, if possible.

> 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.
>
> Example: If the controller is automatically erasing all footage for example within 2 days, a data subject may only get access to that very information [that the material has been deleted] if the request is presented to the controller post those 2 days.

96.

- Article 12 GDPR, excessive requests

97. In case of excessive or manifestly unfounded requests from a data subject, the controller may either charge a reasonable fee in accordance with Article 12 (5) (a) GDPR, or refuse to act on the request (Article 12 (5) (b) GDPR. The controller needs to be able to demonstrate the excessive or manifestly unfounded character of the request.

6.2 Right to erasure and right to object

6.2.1 Right to erasure (Right to be forgotten)

98. If the controller continues to process personal data beyond real-time monitoring (e.g. storing) the data subject may request for the personal data to be erased under Article 17 GDPR.

99. Upon a request, the controller is obliged to erase the personal data without undue delay if one of the circumstances listed under Article 17 (1) GDPR applies (and none of the exceptions listed under Article 17 (3) GDPR does). That includes the obligation to erase personal data when they are no longer needed for the purpose for which they were initially stored, or when the processing is unlawful (see also section 8 on storage periods and obligation to erasure). Furthermore, depending on the legal basis of processing, personal data should be erased:

- *for consent* whenever the consent is withdrawn (and there is no other legal basis for the processing)
- for Legitimate interest:
    - whenever the data subject exercises the right to object (see *section 6.2.2*) and there are no overriding compelling legitimate grounds for the processing, or
    - in case of direct marketing (including profiling) whenever the data subject objects to the processing.

100. If the controller has made the video footage public (e.g. broadcasting or streaming online), reasonable steps need to be taken in order to inform other controllers (that are now processing the personal data in question) of the request pursuant to Article 17 (2) GDPR. The reasonable steps should include technical measures, taking into account available technology and the cost of implementation. To the extent possible, the controller should notify – upon erasure of personal data – anyone to which the personal data previously have been disclosed, in accordance with Article 19 GDPR.

101. Besides the controller's obligation to erase personal data upon the data subject's request, the controller is obliged under the general principles of the GDPR to limit the personal data stored (see *section 8)*.

102. For video surveillance it is worth noticing that by for instance blurring the picture with no retroactive ability to recover the personal data the picture previously contained, the personal data are considered erased in accordance with GDPR.

> Example: A convenience store is having trouble with vandalism in particular on its exterior and is therefore using video surveillance outside of their entrance in direct connection to the walls. A passer-by requests to have his personal data erased from that very moment. The controller is obliged to respond to the request without undue delay and at the latest within one month. Since the footage in question does no longer meet the purpose for which it was initially stored (no vandalism occurred during the time the data subject passed by), there is at the time of the request, no legitimate interest to store the data that would override the interests of the data subjects. The controller needs to erase the personal data.

103.

6.2.2 Right to object

104. For video surveillance based on *legitimate interest* (Article 6 (1) (f) GDPR) or for the necessity when carrying out a task in the *public interest* (Article 6 (1) (e) GDPR) the data subject has the right – at any time –to object, on grounds relating to his or her particular situation, to the processing in accordance

with Article 21 GDPR. Unless the controller demonstrates compelling legitimate grounds that overrides the rights and interests of the data subject, the processing of data of the individual who objected must then stop. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month.

105. In the context of video surveillance this objection could be made either prior to entering, during the time in, or after leaving, the monitored area. 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, or

(2) the monitored area is in such detail restricted so that the controller can assure the approval from the data subject prior to entering the area and it is not an area that the data subject as a citizen is entitled to access.

106. When using video surveillance for direct marketing purposes, the data subject has the right to object to the processing on a discretionary basis as the right to object is absolute in that context (Article 21 (2) and (3) GDPR).

> Example: A company is experiencing difficulties with security breaches in their public entrance and is using video surveillance on the grounds of legitimate interest, with the purpose to catch those unlawfully entering. A visitor objects to the processing of his or her data through the video surveillance system on grounds relating to his or her particular situation. The company however in this case rejects the request with the explanation that the footage stored is needed due to an ongoing internal investigation, thereby having compelling legitimate grounds to continue processing the personal data.

107.

7 TRANSPARENCY AND INFORMATION OBLIGATIONS[18]

108. It has long been inherent to European data protection law that data subjects should be aware of the fact that video surveillance is in operation. They should be informed in a detailed manner as to the places monitored.[19] Under the GDPR the general transparency and information obligations are set out in Article 12 GDPR et seqq. Article 29 Working Party's "Guidelines on transparency under Regulation 2016/679 (WP260)" which were endorsed by the EDPB on May 25th 2018 provide further details. In line with WP260 para. 26, it is Article 13 GDPR, which is applicable if personal data are collected "from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras)".

109. In light of the volume of information, which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency (WP260, par. 35; WP89, p. 22). Regarding video surveillance the most important

18 Specific requirements in national legislation might apply.

19 Article 29 Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance (WP89).

information should be displayed on the warning sign itself (first layer) while the further mandatory details may be provided by other means (second layer).

7.1 First layer information (warning sign)

110. The first layer concerns the primary way in which the controller first engages with the data subject. At this stage, controllers may use a warning sign showing the relevant information. The displayed information may be provided in combination with an icon in order to give, in an easily visible, intelligible and clearly readable manner, a meaningful overview of the intended processing (Article 12 (7) GDPR). The format of the information should be adjusted to the individual location (WP89 p. 22).

7.1.1 Positioning of the warning sign

111. The information should be positioned at a reasonable distance from the places monitored (WP 89, p. 22) in such a way that the data subject can easily recognize the circumstances of the surveillance before entering the monitored area (approximately at eye level). It is not necessary to specify the precise location of the surveillance equipment as long as there is no doubt, as to which areas are subject to monitoring and the context of surveillance is to be clarified unambiguously (WP 89, p. 22). The data subject must be able to estimate which area is captured by a camera so that he or she is able to avoid surveillance or adapt his or her behaviour if necessary.

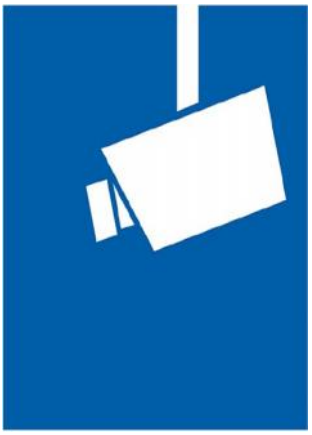
7.1.2 Content of the first layer

112. The first layer information (warning sign) should generally convey the most important information, e.g. the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impacts of the processing.[20] This can include for example the legitimate interests pursued by the controller (or by a third party) and contact details of the data protection officer (if applicable). It also has to refer to the more detailed second layer of information and where and how to find it.

113. In addition the sign should also contain any information that could surprise the data subject (WP260, par. 38). That could for example be transmissions to third parties, particularly if they are located outside the EU, and the storage period. If this information is not indicated, the data subject should be able to trust that there is solely a live monitoring (without any data recording or transmission to third parties).

20 See WP260, par. 38

Example:



Video surveillance!

Identity of the controller and, where applicable, of the controller's representative:

Contact details of the data protection officer (where applicable):

Purposes of the processing for which the personal data are intended as well as the legal basis for the processing:

Further information is available:
- via notice
- at our reception/ customer information/ register
- via internet (URL)...

Data subjects rights: As a data subject you have several rights against the controller, in particular the right to request from the controller access to or erasure of your personal data.

For details on this video surveillance including your rights, see the full information provided by the controller through the options presented on the left.

114.

7.2 Second layer information

115. The second layer information must also be made available at a place easily accessible to the data subject, for example as a complete information sheet available at a central location (e.g. information desk, reception or cashier) or displayed on an easy accessible poster. As mentioned above, the first layer warning sign has to refer clearly to the second layer information. In addition, it is best if the first layer information refers to a digital source (e.g. QR-code or a website address) of the second layer. However, the information should also be easily available non-digitally. In any case, it must be possible to access the second layer information without entering the surveyed area. This can be achieved for example by a link or any other appropriate means like a phone number that can be called. It must contain all other information that is mandatory under Article 13 GDPR.

116. In addition to these options, and also to make them more effective, the EDPB promotes the use of technological means to provide information to data subjects. This may include for instance; geolocating cameras and including information in mapping apps or websites so that individuals can easily, on the one hand, identify and specify the video sources related to the exercise of their rights, and on the other hand, obtain more detailed information on the processing operation.

Example: A shop owner is monitoring his shop. To comply with Article 13 it is sufficient to place a warning sign at an easy visible point at the entrance of his shop, which contains the first layer information. In addition, he has to provide an information sheet containing the second layer information at the cashier or any other central and easy accessible location in his shop.

117.

8 STORAGE PERIODS AND OBLIGATION TO ERASURE

118. Personal data may not be stored longer than what is necessary for the purposes for which the personal data is processed (Article 5 (1) (c) and (e) GDPR). In some member states, there may be specific provisions for storage periods with regards to video surveillance in accordance with Article 6 (2) GDPR.

119. Whether the personal data is necessary to store or not, should be controlled within a narrow timeline. In general, legitimate purposes for video surveillance are often property protection or preservation of evidence. Usually damages that occurred can be recognized within one or two days. Taking into consideration the principles of Article 5 (1) (c) and (e) GDPR, namely data minimization and storage limitation, the personal data should in most cases (e.g. for the purpose of detecting vandalism) be erased, ideally automatically, after a few days. The longer the storage period is set (especially when beyond 72 hours), the more argumentation for the legitimacy of the purpose and the necessity of storage has to be provided. If the controller uses video surveillance not only for monitoring its premises but also intends to store the data, the controller must assure that the storage is actually necessary in order to achieve the purpose. If so, the storage period needs to be clearly defined and individually set for each particular purpose. It is the controller's responsibility to define the retention period in accordance with the principles of necessity and proportionality and to demonstrate compliance with the provisions of the GDPR.

> Example: An owner of a small shop would normally take notice of any vandalism the same day. In consequence, a regular storage period of 24 hours is sufficient. Closed weekends or holidays might however be reasons for a longer storage period. If a damage is detected he may also need to store the video footage a longer period in order to take legal action against the offender.

120.

9 TECHNICAL AND ORGANISATIONAL MEASURES

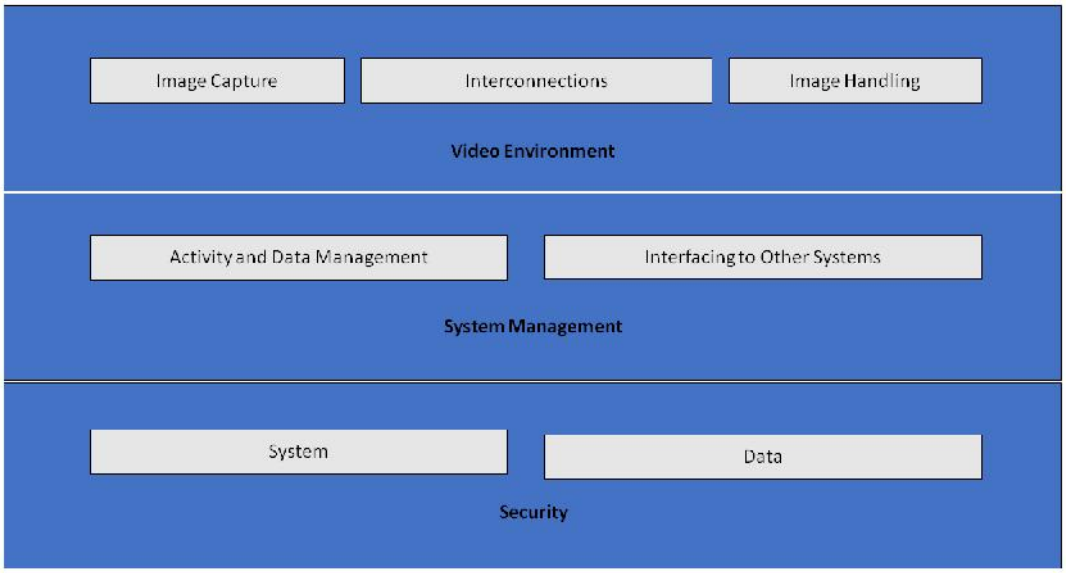
121. As stated in Article 32 (1) GDPR, processing of personal data during video surveillance must not only be legally permissible but controllers and processors must also adequately secure it. Implemented **organizational and technical measures** must be **proportional to the risks to rights and freedoms of natural persons**, resulting from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to video surveillance data. According to Article 24 and 25 GDPR, controllers need to implement technical and organisational measures also in order to safeguard all data-protection principles during processing, and to establish means for data subjects to exercise their rights as defined in Articles 15 – 22 GDPR. Data controllers should adopt internal framework and policies that ensure this implementation both at the time of the determination of the means for processing and at the time of the processing itself, including the performance of data protection impact assessments when needed.

9.1 Overview of video surveillance system

A video surveillance system (VSS)21 consists of analogue and digital devices as well software for the purpose of capturing images of a scene, handling the images and displaying them to an operator. Its components are grouped into the following categories:

- Video environment: image capture, interconnections and image handling
  - the purpose of image capture is generation of an image of the real world in such format that it can be used by the rest of the system
  - interconnections describe all transmission of data within the video environment, i.e. connections and communications. Examples of connections are cables, digital networks, and wireless transmissions. Communications describe all video and control data signals, which could be digital or analogue
  - image handling includes analysis, storage and presentation of an image or a sequence of images
- From the system management perspective, a VSS has the following logical functions:
  - data management and activity management, which includes handling operator commands and system generated activities (alarm procedures, alerting operators)
  - interfaces to other systems might include connection to other security (access control, fire alarm) and non-security systems (building management systems, automatic license plate recognition)
- VSS security consists of system and data confidentiality, integrity and availability
  - system security includes physical security of all system components and control of access to the VSS
  - data security includes prevention of loss or manipulation of data

21 GDPR does not provide a definition for it, a technical description can for example be found in EN 62676-1-1:2014 Video surveillance systems for use in security applications – Part 1-1: Video system requirements.



122.

Figure 1- video surveillance system

9.2 Data protection by design and by default

123. As stated in Article 25 GDPR, controllers need to implement appropriate data protection technical and organisational measures as soon as they plan for video surveillance, before they start the collection and processing of video footage. These principles emphasize the need for built-in privacy enhancing technologies, default settings that minimise the data processing, and the provision of the necessary tools that enable the highest possible protection of personal data[22].

124. Controllers should build data protection and privacy safeguards not only into the design specifications of the technology but also into organisational practices. When it comes to organizational practices, the controller should adopt an appropriate management framework, establish and enforce policies and procedures related to video surveillance. From the technical point of view, system specification and design should include requirements for processing personal data in accordance with principles stated in Article 5 GDPR (lawfulness of processing, purpose and data limitation, data minimisation by default in the sense of Article 25 (2) GDPR, integrity and confidentiality, accountability etc.). In case a controller plans to acquire a commercial video surveillance system, the controller needs to include these requirements in the purchase specification. The controller needs to ensure compliance with these requirements applying them to all components of the system and to all data processed by it, during their entire lifecycle.

9.3 Concrete examples of relevant measures

125. Most of the measures that can be used to secure video surveillance, especially when digital equipment and software are used, will not differ from those used in other IT systems. However, regardless of the solution selected, the controller must adequately protect all components of a video surveillance

22 WP Opinion 168 on the "The Future of Privacy", joint contribution by the Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (adopted on 01 December 2009), https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

system and data under all stages, i.e., during storage (data at rest), transmission (data in transit) and processing (data in use). For this, it is necessary that controllers and processors combine organizational and technical measures.

126. When selecting technical solutions, the controller should consider privacy-friendly technologies also because they enhance security. Examples of such technologies are systems that allow masking or scrambling areas that are not relevant to surveillance, or the editing out of images of third persons, when providing video footage to data subjects.[23] On the other hand, the selected solutions should not provide functions that are not necessary (e.g., unlimited movement of cameras, zoom capability, radio transmission, analysis and audio recordings). Functions provided, but not necessary, must be deactivated.

127. There is a lot of literature available on this subject, including international standards and technical specifications on the physical security of multimedia systems[24], and the security of general IT systems[25]. Therefore, this section provides only a high-level overview of this topic.

9.3.1 Organisational measures

128. Apart from a potential DPIA needed (see section 10), controllers should consider the following topics when they create their own video surveillance policies and procedures:

- Who is responsible for management and operation of the video surveillance system
- Purpose and scope of the video surveillance project
- Appropriate and prohibited use (where and when video surveillance is allowed and where and when it is not; e.g. use of hidden cameras and audio in addition to video recording[26])
- Transparency measures as referred to in section 7 (Transparency and information obligations)
- How video is recorded and for what duration, including archival storage of video recordings related to security incidents
- Who must undergo relevant training and when
- Who has access to video recordings and for what purposes
- Operational procedures (e.g. by whom and from where video surveillance is monitored, what to do in case of a data breach incident)
- What procedures external parties need to follow in order to request video recordings, and procedures for denying or granting such requests
- Procedures for VSS procurement, installation and maintenance
- Incident management and recovery procedures.

---

23 The use of such technologies may be even mandatory in some cases to comply with Article 5 (1) (c). In any case they can serve as best practice examples.

24 IEC TS 62045 — Multimedia security - Guideline for privacy protection of equipment and systems in and out of use

25 ISO/IEC 27000 — Information security management systems series

26 This may depend on national laws and sector regulations

9.3.2 Technical measures

129. S**ystem security** means **physical security** of all system components, system integrity i.e. **protection against and resilience under intentional and unintentional interference with its normal operations** and **access control**. Data security means **confidentiality** (data is accessible only to those who are granted access), **integrity** (prevention against data loss or manipulation) and **availability** (data can be accessed when it is required).

130. **Physical security** is a vital part of data protection and the first line of defence, because it protect VSS equipment from theft, vandalism, natural disaster, manmade catastrophes and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). In case of an analogue based systems, physical security plays the main role in their protection.

131. **System and data security,** i.e. protection against intentional and unintentional interference with its normal operations may include:

- Protection of the entire VSS infrastructure (including remote cameras, cabling and power supply) against physical tampering and theft
- Protection of footage transmission with communication channels secure against interception
- Data encryption
- Use of hardware and software based solutions such as firewalls, antivirus or intrusion detection systems against cyber attacks
- Detection of failures of components, software and interconnections
- Means to restore availability and access to the system in the event of a physical or technical incident.

Access control ensures that only authorized people can access the system and data, while others are prevented from doing it. Measures that support physical and logical access control include:

- Ensuring that all premises where monitoring of video surveillance is done and video footage is stored are secured against unsupervised access by third parties
- Positioning monitors in such a way (especially when they are in open areas, like a reception) so that only authorized operators can view them
- Procedures for granting, changing and revoking physical and logical access are defined and enforced.
- Methods and means of user authentication and authorization including e.g. passwords length and change frequency are implemented.
- User performed actions (both to the system and data) are recorded and regularly reviewed.
- Monitoring and detection of access failures is done continuously and identified weaknesses are addressed as soon as possible.

10 DATA PROTECTION IMPACT ASSESSMENT

132. According to Article 35 (1) GDPR controllers are required to conduct data protection impact assessments (DPIA) when a type of data processing is likely to result in a high risk to the rights and

freedoms of natural persons. Article 35 (3) (c) GDPR stipulates that controllers are required to carry out data protection impact assessments if the processing constitutes a systematic monitoring of a publicly accessible area on a large scale. Moreover, according to Article 35 (3) (b) GDPR a data protection impact assessment is also required when the controller intends to process special categories of data on a large scale.

133. The Guidelines on Data Protection Impact Assessment[27] provide further advice, and more detailed examples relevant to video surveillance (e.g., concerning the "use of a camera system to monitor driving behaviour on highways"). Article 35 (4) GDPR requires that each supervisory authority publish a list of the kind of processing operations that are subject to mandatory DPIA within their country. These lists can be usually found on the authorities' websites. Given the typical purposes of video surveillance (protection of people and property, detection, prevention and control of offences, collection of evidence and biometric identification of suspects), it is reasonable to assume that many cases of video surveillance will require a DPIA. Therefore, data controllers should carefully consult these documents in order to determine whether such an assessment is required and conduct it if necessary. The outcome of the performed DPIA should determine the controller's choice of implemented data protection measures.

134. It is also important to note that if the results of the DPIA indicate that processing would result in a high risks despite security measures planned by the controller, then it will be necessary to consult the relevant supervisory authority prior to the processing. Details on prior consultations can be found in Article 36.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

27 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, wp248rev.01, http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236