The General Data Protection Regulation

Videosurveillance guidelines

Date of first adoption: 13/08/2018

Date of update: 19/04/2024

Content

Introduction 2
1. Principle of lawfulness of processing 3
2. Principle of purpose 5
3. Principle of transparency 6
3.1. First level of information 6
3.2. Second level of information 7
4. Principle of necessity and proportionality (data minimisation) 9
4.1. Limited field of view of cameras filming the interior, exterior or surroundings of a building or site 9
4.2. Permanent and continuous monitoring 9
4.3. Monitoring of employee performance and/or behaviour 10
4.4. Places reserved for employees for private use 11
4.5. Examples of video surveillance areas 11
4.6. Processing of sounds associated with images 13
5. Principle of storage limitation 14
6. Article L. 261-1 of the Labour Code: **specific legal** provisions concerning the processing of data for supervisory purposes in the context of employment relationships. 15
7. Should a data protection impact assessment ('DPIA') be carried out in relation to video surveillance? 16
8. Other obligations under the GDPR 17

Introduction

On 25th May 2018, the GDPR[1] has come into effect. One of the direct consequences of the GDPR is that it is no **longer necessary to seek prior authorisation** from the CNPD to install a CCTV system.

Although the obligation to request prior authorisation from the CNPD has been repealed, controllers who install or have installed CCTV are obliged to comply with the principles and obligations deriving from the GDPR, including the obligation to keep a register of the processing of personal data that is carried out under their responsibility.[2] The processing of personal data resulting from video surveillance will therefore have to be included in this register and include all the information required by Article 30 of the GDPR.

Moreover, contrary to the amended law of 2 August 2002[3] (repealed), the GDPR no longer defines the concept of "surveillance". Nevertheless, the installation of a CCTV system aimed at employees is still to be regarded as the processing of personal data for surveillance purposes in the context of employment relationships within the meaning of Article L. 261-1 of the Labour Code, which must be complied with by the employer.

Without wishing to be exhaustive, the CNPD would also like to **recall some of the principles and obligations** applicable to video surveillance.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR').
[2] *cf.* Article 30 GDPR.
[3] Amended Law of 2 August 2002 on the protection of individuals with regard to the processing of personal data, repealed by the Law of 1 August 2018 on the organisation of the National Commission for Data Protection and the General Data Protection Regime.

1. Principle of lawfulness of processing

Any processing of personal data must be based on one of the conditions of lawfulness exhaustively listed in Article 6.1[4] of the GDPR. In the context of a CCTV system, the most appropriate condition of lawfulness will generally be that of processing necessary for the purposes of the controller's legitimate interests, unless the interests or fundamental rights and freedoms of the persons subject to video surveillance prevail (Article 6.1(f) GDPR). The CNPD points out that, in order to be able to use the condition of lawfulness constituted by the legitimate interest, three cumulative conditions must be met:

(1) the existence of a valid legitimate interest (for example, the desire to protect one's property against theft or one's employees against physical harm);[5]

(2) the need to process personal data for the purposes pursued by the legitimate interest invoked (i.e. are there reasonable and less privacy-intrusive alternative means to achieve the same purpose?); and

(3) the fact that the fundamental rights and interests of data subjects must not prevail over the legitimate interests of the controller ('the balancing exercise').

That third condition consists in verifying whether video surveillance is likely to infringe the fundamental rights and interests of data subjects, and if so, whether those fundamental rights and interests must not prevail over the controller's interest in setting up a video surveillance system – in which case setting up is not permitted.[6]

In most cases, the fundamental rights and freedoms of data subjects will prevail over the legitimate interests pursued by the controller where video surveillance presents risks of a high level of interference with the rights of data subjects or in areas where there is a reasonable expectation not to be subject to surveillance. Examples of such areas are given in section 4.5.B. below. The balancing exercise must in any event be carried out on a case-by-case basis.

Controllers must be able to explain the choices made regarding the location of cameras, the areas monitored and the technical means used.

Attention: In principle, consent[7] does not constitute an appropriate basis for the lawfulness of video surveillance.

By their nature, video surveillance systems have, in their field of vision, an indeterminate number of persons simultaneously.[8] In principle, it is not possible for the controller to seek the consent of each of the persons passing through the camera's field of view, nor to prove that each data subject has given their consent before their personal data are processed.[9]

[4] *cf.* Article 6.1(a) – (f) GDPR.
[5] In such a case, it is recommended to document the fact that a robbery or assault has already taken place (e.g. by keeping a copy of a complaint filed with the police), in order to prove that a real interest exists.
[6] For more information on the legitimate interest and the analysis to be carried out, the CNPD refers to paragraphs 17 to 40 of Guidelines 3/2019 of the European Data Protection Board on the processing of personal data by video devices, available at the following address: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.
[7] *See Article* 6.1(a) of the GDPR.
[8] See in this regard paragraphs 43 to 48 of the European Data Protection Board's Guidelines 3/2019 on the processing of personal data by video devices, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.
[9] *cf.* Article 7.1 of the GDPR.

Moreover, in the event that the data subject withdraws their consent, the controller will find it difficult to demonstrate that the personal data is no longer processed.[10]

Obtaining a valid consent by the controller is made even more difficult when the CCTV cameras have employees of the controller in their field of vision. Indeed, one of the conditions to be met for consent to be valid – which stem from Article 4. 11) GDPR – is that it was freely given by the data subject. In the context of employment relationships, given the dependence and imbalance of powers that may exist in 'employer-employee' relationships, employees are only very rarely able to refuse or revoke their consent without fear of adverse consequences.

In those circumstances, consent can very rarely be regarded as freely given.[11]

[10] cf Article 7(3) of the GDPR.

[11] See in this regard paragraph 21 et seq. of the European Data Protection Board's Guidelines 5/2020 on consent within the meaning of Regulation (EU) 2016/679, taken up by the European Data Protection Board, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. See also Section 6.2 of Opinion 2/2017 of the Article 29 Working Party on data processing at the workplace (WP 249), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

2. Principle of purpose

According to Article 5(1)(b) of the GDPR, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes.

For example, video surveillance may have the following purposes:

- secure access to the building;
- ensure the safety of staff and customers;
- detect and identify potentially suspicious or dangerous behaviour likely to cause accidents or incidents;
- accurately identify the origin of an incident;
- protecting assets (buildings, facilities, equipment, merchants, cash, etc.);
- organising and supervising the rapid evacuation of persons in the event of an incident;
- to be able to alert the emergency, fire or law enforcement services in good time and to facilitate their intervention.
- ...

On the other hand, the CNPD is generally of the opinion that the following purposes cannot be pursued by a controller using a CCTV system, since such a system installed for these purposes would not comply with the principles defined below in point 4:

- check that employees are working and not spending too much time on their phones or chatting with colleagues;
- checking that employees are complying with working hours;
- verify that employees comply with the work instructions given;
- verify that employees are behaving appropriately with customers.

Before installing a CCTV system, the controller must define precisely the purpose(s) he/she actually wishes to pursue by using such a system, and may not subsequently use it for any other purpose. Thus, an employer who decides, for example, to install a CCTV system for the sole purpose of ensuring the safety of staff and customers, may not then use it for another purpose for which the data was not initially collected and used and which, in particular, was not brought to the attention of employees.

Cameras that are used for the same purposes by a single controller may be jointly documented.

The example given below in point 4.3 of these guidelines illustrates this principle of purpose limitation.

3. Principle of transparency

Any controller shall be obliged to provide information to the data subjects of the processing of personal data which it carries out. This information must meet the requirements of Articles 12 and 13 of the GDPR.

In accordance with Article 12(1) of the GDPR, the provision of information to data subjects and communications addressed to them must be carried out in a 'concise, *transparent, intelligible and easily accessible* manner, *in clear and plain language'.*

The word 'provide' is crucial here and it 'means *that the controller must take concrete steps to provide the information in question to the data subject or to actively direct the data subject to the location of that information (e.g. by means of a direct link, QR code, etc.)'.* [12]

In order to make it easier for data subjects to understand the processing of data carried out when using a CCTV system, the EDPB Guidelines on the processing of personal data by video devices[13] suggest a two-tier approach.

Such an approach consists in providing – as a first step – a series of information to data subjects via, for example, billboards (see point 3.1. The first level of information), and then – as a second step – to communicate via other means, all the information required under Article 13 of the GDPR (see point 3.2. The second level of information).

Attention: If the video surveillance targets employees of the controller, the CNPD draws the attention of the controllers to the additional obligations, in particular as regards collective information, provided for in Article L. 261-1 of the Labour Code (see point 5. below).

In that regard, it should also be pointed out that employees must be informed individually and that the mere fact that the staff delegation is informed does not ensure that employees have been informed individually of the precise elements of Article 13(1) and (2) of the GDPR.[14]

3.1. First level of information

In order to inform the data subjects of the presence of a CCTV system, the CNPD recommends communicating, for example via billboards, a first level of information containing:

- the identity and contact details of the controller;
- the purpose(s) of the processing;
- information with the greatest influence on the data subject (e.g. retention period of images, live monitoring, publication or transmission of video footage to third parties;
- the existence of the rights available to the data subjects;
- a statement that more complete information exists (second level of information) and the means of accessing it (e.g. a hyperlink to the controller's website, the use of a QR code, a telephone number to call or an indication of where this more detailed information is available.

[12] See in this regard point 33 of the Guidelines of the Article 29 Working Party on transparency within the meaning of Regulation (EU) 2016/679 (WP260rev. 01), taken over by the European Data Protection Board.
[13] Guidelines3/2019 of the European Data Protection Board on the processing of personal data by video devices, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.
[14] *See Decision* 14FR/2021 of 12 May 2012 of the Restricted Panel of the National Commission for Data Protection, paragraph 47.

These information signs must be displayed visibly (i.e. a sign of sufficient size) at all times at the main entrances and exits or in the vicinity of the site subject to video surveillance and must be easily legible at head height. The data subjects must in principle be able to acquaint themselves with it before entering the supervised area. For a quick and easy warning of the persons concerned, the billboard is ideally accompanied by pictograms.

Example of a billboard[15]

<table>
<tr><td rowspan="2">
</td><td>Identity of the controller:

Contact details of the controller</td></tr>
<tr><td>Purpose(s) pursued by video surveillance:

Information with the greatest influence on the data subject
(e.g. image retention period, live monitoring, publication or transmission of video footage to third parties)</td></tr>
<tr><td>More information on this video surveillance is available:
- via our information notice;
- on our website [hyperlink to the website of the controller];
- [insert QR Code]
- by phone
- ...</td><td>Rights of data subjects:

The GDPR gives you as a data subject rights to control the use of your own data.
In particular, you have a right of access and a right to erasure.

For more information on your rights, please follow the [link/QR code/info leaflet]</td></tr>
</table>

3.2. Second level of information

The second level of information must contain, in detail, all the information required by Article 13 of the GDPR. It must meet the standards of Article 12 GDPR, and must therefore be drafted in a concise, transparent, comprehensible manner, and in clear and plain language. The second level of information must be made available in a place easily accessible by the data subject. It could possibly be provided or made available by other means, such as a copy of the privacy policy sent by e-mail to employees or a link on the website to an information notice for non-employees.[16] A non-digital version should always be available to the data subject, for example via an explanatory document, which is made available by the controller.

[15] **Attention:** This document is a (non-binding) example of the first-level information. The various sections must be completed and adapted according to the video surveillance system implemented by the controller.
[16] *See Decision* 14FR/2021 of 12 May 2021 of the Restricted Formation of the National Commission for Data Protection, paragraph 54.

For more information on the principle of transparency in video surveillance, please refer to point 7 of EDPB Guidelines 3/2019 on the processing of personal data by video devices.[17]

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

4. Principle of necessity and proportionality (data minimisation)

The principle of necessity implies, first of all, that a controller must have recourse to a video surveillance device only where there are no alternative means less intrusive on the privacy of data subjects to achieve the intended purpose.

The principle of data minimisation in the field of video surveillance further implies that when a video surveillance system is installed, it must film only what is strictly necessary to achieve the purpose(s) pursued ('adequate, relevant and limited to what is necessary') and that processing operations must not be disproportionate to that purpose.

By way of illustration, an overview of areas where the CNPD considers that a CCTV system may or may not be problematic is given below in section 4.5. However, it is necessary to carry out a case-by-case analysis of the situation in order to analyse the necessity and proportionality of video surveillance, in particular in the light of criteria such as, for example, the nature of the place to be placed under video surveillance, its situation, its configuration or its attendance.

4.1. Limited field of view of cameras filming the interior, exterior or surroundings of a building or site

Cameras intended to monitor a place of access (entrance and exit, threshold, stairway, door, awning, hall, etc.) must have a field of view limited to the area strictly necessary to visualise the persons preparing to access it; those filming external accesses shall not mark the entire width of a sidewalk, if any, along the building or adjacent public roads.

Similarly, exterior cameras installed in or around a building must be configured in such a way that they do not capture the public road or the approaches, entrances, accesses and interiors of other neighbouring buildings which may fall within their field of vision.

Depending on the configuration of the premises, it is sometimes impossible to install a camera that does not include in its field of vision part of the public road, approaches, entrances, accesses and interiors of other buildings.[18] In such a case, the CNPD considers that the controller must implement masking or blurring techniques in order to limit the field of vision to its property.

4.2. Permanent and continuous monitoring

- **Supervision of non-employees**

Permanent supervision of non-employees is not always permitted. For example, the CNPD considers it disproportionate to film the interior of a dining room with tables. The same applies to the terrace or counter of a café. Although there may be a certain risk of theft or vandalism in such places, it considers that the customers present will, on a permanent basis, be subject to video surveillance even though they choose a restaurant or café as a meeting place to have a good time around a meal, to chat, to have fun or to relax. Customers who stay in this type of place for a longer or shorter period of time must be able to legitimately expect not to be filmed during these private moments. The use of cameras in the dining room including the

[18] Decision *27FR/2021* of 15 July 2021 of the Restricted Panel of the National Commission for Data Protection, paragraphs 47-49.

tables is likely to film the behaviour of each customer sitting at a table and may create discomfort or even psychological pressure for customers who feel observed throughout their presence in the restaurant. Such permanent monitoring must therefore be regarded as disproportionate to the intended purpose and constitutes an infringement of the customer's private sphere.

- **Supervision of employees**

In the workplace,employees have in principle the right not to be subject to continuous and permanent supervision.

Compliance with the principle of proportionality means that the employer must have recourse to the means of supervision most protective of the employee's private sphere. Compliance with this principle requires that, for example, automatic and continuous monitoring of employees should be avoided.

Thus, for example, the operator of a restaurant could not monitor his employees inside the kitchen, relying on the protection of his property. Employees would be subject to video surveillance almost permanently and it is clear that such surveillance can create significant psychological pressure for employees who feel and know that they are being observed, especially as the surveillance measures last over time. The same applies, for example, to the video surveillance of the interior of an office, an open-space, or a workshop in which one or more employees work permanently. Permanent supervision is considered disproportionate to the intended purpose and constitutes an excessive interference with the private sphere of the employee employed at his or her workstation. In this case, the fundamental rights and freedoms of employees must prevail over the legitimate interests pursued by the employer.

In order to avoid permanent and continuous surveillance, the controller must limit the field of vision of the cameras to the only surface necessary to achieve the intended purposes.

Thus, by way of example, the purpose of camera surveillance of a cash register in a shop may be to protect the controller's assets against acts of theft committed by its employees or by a customer/user and to ensure the safety of its staff. However, in order not to infringe the privacy of employees, the camera should be configured so that employees behind a cash desk are not targeted, by directing its field of view towards the cash desk itself and the front of the counter, i.e. the waiting area of customers in front of the counter, in order to allow the identification of perpetrators, for example.

4.3. Monitoring of employee performance and/or behaviour

The CNPD considers that video surveillance should not be used to observe the behaviour and performance of the controller's staff members outside the purposes for which it was set up.

Thus, an employer has the right to use images of an employee who commits theft of goods and which come from a video surveillance system used for the purpose of protecting property. However, he does not have the right to use the camera in order to find that an employee is talking too long with a client or a co-worker, or to then use the recordings as evidence, in order to take disciplinary measures against that employee. This would constitute a misuse of purpose prohibited by the GDPR.

4.4. Places reserved for employees for private use

The CNPD considers that surveillance cameras must not film areas reserved for employees for private use or which are not intended for the performance of work tasks, such as toilets, changing rooms, smoking areas, rest areas, the room made available to the staff delegation, the kitchen/kitchenette, etc.

4.5. Examples of video surveillance areas

The examples of areas below should be read and considered together with points 4.1 to 4.4 above.

A. Areas where the installation of video surveillance is in principle proportionate:

- all types of access, limiting the fields of vision of the cameras to the area strictly necessary to visualise the persons preparing to access them. Cameras must not target public roads or unnecessary spaces, even in an ancillary manner, such as a pointer;[19]
- storage rooms for goods/reserves/warehouses/storage halls or sheds (unless employees are permanently assigned to work in the stock, such as storekeepers);
- sales areas or areas of a shop/shop shelves/shopping arcade/exhibition area/sales and consultancy area (except permanent workstations behind a counter);
- a car park (indoor/outdoor/underground);
- delivery or loading areas/delivery and unloading platforms;
- a computer room/server room;
- an automatic car wash/carwash;
- a petrol pump;
- a safe / secure room / automatic deposit boxes;
- cash-in-transit premises / van room;
- technical installations or production machinery (provided that permanent workstations are not filmed);
- the technical room of a building/maintenance room/counter room of a condominium;
- archive premises;
- ATMs/banking machines.

[19] *See* Decision 27FR/2021 of 15 July 2021 of the Restricted Panel of the National Commission for Data Protection, paragraphs 47-49.

B. Areas where the installation of video surveillance is in principle disproportionate:

- a public road / sidewalk (except in exceptional cases depending on the specific configuration of the premises; the field of vision may, however, encompass only an extremely limited part of the public road);
- the interior of a consumption area of a restaurant, a bar, a nightclub, etc. (catering room, consumption counter, terrace, canteen/cafeteria, etc.);
- the interior of a restaurant kitchen;
- the private entrance of a dwelling into a condominium building;
- a neighbouring land or building;
- the interior of an office with a permanent workstation;
- a rest or living room;
- the interior of a wellness area (sauna, deckchairs, etc.)
- training areas in a gym;
- toilets / showers;
- an office of the staff representative or its access (if it leads only to that office);
- a kitchenette;
- a smoking area;
- a cloakroom / locker room / fitting room;
- a garage workshop / a tyre assembly and dismantling workshop / a production workshop / a workshop;
- the hairdressing area of a hairdressing salon;
- the play area of a crèche.

C. Areas where the proportionality of video surveillance depends on the circumstances of the case and the measures put in place to ensure privacy

Video surveillance of the areas listed below may be permitted in some cases and not permitted in other cases. Whether or not video surveillance of such areas is proportionate will depend on the circumstances of the case, such as the nature, location or configuration of the premises, the nature of the activity carried out by the controller and the risks inherent in that activity, etc. It will also depend on the measures taken by the controller to make video surveillance less invasive of the privacy of data subjects (e.g. limiting the field of vision of cameras, using masking/cutting techniques, etc.). A case-by-case analysis must be carried out by the controller.

- the surroundings of a building;
- a waiting room;

- counters;
- a reception desk/reception desk;
- cash registers;
- a cash-counting room / a cash-processing room;
- the common parts of a building in co-ownership;
- the playground of a school (and its surroundings);
- a swimming pool;
- the roof of a building;
- a meeting room.

4.6. Processing of sounds associated with images

Surveillance by means of video cameras shall only cover images excluding sounds. Live listening and recording of the sound associated with the images makes video surveillance even more intrusive and must be regarded as disproportionate.

5. Principle of storage limitation

The GDPR stipulates that personal data must be kept in a form that allows the identification of data subjects for no longer than is necessary for the purposes for which they are processed. As regards to video surveillance, the CNPD considers that images can be kept in principle for up to 8 days.

The controller may exceptionally retain the images for a period of 30 days. However, the reasons justifying such a retention period must be indicated in the register of processing operations.

A shelf life of more than 30 days is generally considered disproportionate.[20]

In the event of an incident or offence, the images may be retained beyond the aforementioned time limits, as part of the transmission of data to the competent judicial authorities and law enforcement authorities competent to detect or prosecute criminal offences.

Finally, the controller must ensure that the images are destroyed after the retention period has expired. The introduction of automatic erasure is recommended by the CNPD.

[20] *See Decision* 14FR/2021 of 12 May 2021 of the Restricted Formation of the National Commission for Data Protection, paragraph 38.

6. Article L. 261-1 of the Labour Code: **specific legal** provisions concerning the processing of data for supervisory purposes in the context of employment relationships

An employer wishing to install video surveillance must, **in addition to complying with points 1-4 above and points 6-7 below,** ensure compliance with the **specific rules of Article L. 261-1 of the Labour Code.**

Article L. 261-1 of the Labour Code allows the processing of personal data for the purpose of monitoring employees in the context of employment relationships, by the employer, solely on the basis of **one of the conditions of lawfulness exhaustively listed** in Article 6.1(a) to (f) of the GDPR (see point 1.).

For such processing of personal data, including video surveillance at the workplace, Article L. 261-1 of the Labour Code provides for an **obligation of prior collective information** with regard to staff representation, in addition to **the individual information of employees** in Articles 12 and 13 of the GDPR. This information **must contain:**

- a detailed description of the purpose of the intended processing,
- a detailed description of how the monitoring system is to be implemented,
- where applicable, the duration or criteria for the retention of the data, and
- a formal undertaking by the employer that the data collected will not be used for a purpose other than that explicitly provided for in the prior information.

Article L. 261-1 of the Labour Code provides that, except where the processing of personal data for supervisory purposes meets a legal or regulatory obligation, the provisions laid down in Articles L. 211-8 and L.414-9 of the Labour Code apply, where the processing is carried out for the following purposes:

1. for the safety and health needs of employees, or

2. for the control of the production or benefits of the employee, where such a measure is the only means of determining the exact salary, or

3. within the framework of a working organisation based on flexitime in accordance with the Labour Code.

In all cases of data processing projects for the purpose of monitoring employees in the context of employment relationships, the staff delegation, or failing that the employees concerned, may, within 15 days of the prior information referred to above, submit a **request for a prior opinion** on the compliance of the processing project to the CNPD, which must take a decision within one month of the referral. The request shall have suspensive effect during that period.

Finally, Article L. 261-1 of the Labour Code states that the employees concerned always have **the right to lodge a complaint** with the CNPD in the event of infringement of their rights, such a complaint constituting neither a serious ground nor a legitimate ground for dismissal.

7. Should a data protection impact assessment ('DPIA') be carried out in relation to video surveillance?

Article 35 of the GDPR requires a "DPIA" to be carried out "where *a type of processing, in particular through the use of new technologies, and taking into account the nature, scope, context and purposes of the processing,* ***is likely to result in a high risk*** *to the rights and freedoms of natural persons".*

Article 35(3) of the GDPR also provides for three cases in which a 'DPIA' is particularly required. One of these three cases concerns the 'systematic *large-scale monitoring of a publicly accessible area'.* In some situations, the installation of a video surveillance system could fall in this case.

In addition, the European Working[21] Group (G29) Guidelines on Data Protection Impact Assessment (DPIA) specify the 9 criteria to be taken into account when assessing whether a data processing operation is likely to result in a high risk to the rights and freedoms of natural persons, and therefore whether or not to carry out a DPIA. Depending on the location and context in which video surveillance cameras are implemented, several of these criteria could be met, such as the processing of 'data *concerning vulnerable persons'* (employees, children, the elderly, etc.), large-scale collection, 'systematic *monitoring'* or the criterion of 'innovative *use or application of technological or organisational solutions'.*

The CNPD would also like to draw the attention of controllers to Guidelines 3/2019 on the processing of personal data by video devices, which state that:

> *"Given the common purposes of video surveillance (protection of persons and property, detection, prevention and control of offences, collection of evidence and biometric identification of suspects), it is reasonable to assume that a data protection impact assessment will be necessary in many cases of use of video surveillance. Therefore, it is up to the controllers to carefully consult those documents in order to determine whether an impact assessment should be provided for and to carry it out if necessary.*
>
> *The result of the analysis carried out should guide the choice of the controller as to the data protection measures implemented. »*[22]

[21] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and how to determine whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679 (WP 248 rev.01), available at: https://ec.europa.eu/newsroom/article29/items/611236

[22] Point 137 of the European Data Protection Board Guidelines 3/2019 on the processing of personal data by video devices. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

8. Other obligations under the GDPR

In addition to the principles set out in these guidelines, all the provisions of the GDPR remain, of course, applicable to the processing of personal data that constitutes video surveillance.

Thus, the CNPD wishes to recall, in particular, that if the controller uses a service provider to install or manage the video surveillance device (for example, a security company), that service provider will be regarded as a processor within the meaning of Article 4(8) of the GDPR, if it processes personal data on behalf of the controller. In this case, a **subcontract** meeting the criteria of Article 28 of the GDPR will have to be concluded between the controller and the processor.

Furthermore, the CNPD wishes to draw the attention of controllers and processors to the obligation stemming from Article 32 of the GDPR to put in place adequate **technical and organisational measures** to ensure the security and confidentiality of the data undergoing processing. This means in particular that:

- access to the data collected via the video-surveillance system must be limited only to persons who, in the course of their duties, have a legitimate need to have access to them, in view of the purposes pursued.
- access to the data must be secure (e.g. with a strong password and login) and each person with access to the data must have an individual access account. An access log must also be available, so that it is possible to trace the persons who accessed the data, as well as the data that were accessed by those persons, in the event of abuse.

For further recommendations, including on the rights of data subjects, the CNPD refers to the EDPS Guidelines 3/2019 on the processing of personal data by video devices.[23]

In addition, the CNPD would like to recall that if a subcontractor is involved (e.g. a security company) in the context of video surveillance, a subcontract meeting the criteria of Article 28 GDPR will have to be concluded. Further information on subcontracting is available on the CNPD website.[24]

Finally, the CNPD wishes to draw the attention of controllers to the importance of the question of the country in which the images captured by the video surveillance system are stored, whether this storage is carried out by the controller himself or by his processor (e.g. in the event of recourse to a processor offering a solution with storage of images in the cloud). Indeed, if the images are transferred to a country outside the European Union, the controller must comply with the GDPR requirements for data transfers to third countries. More information is available on the CNPD website.[25]

[23] Guidelines 3/2019 of the European Data Protection Board on the processing of personal data by video devices, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.
[24] https://cnpd.public.lu/en/professionals/obligations/subcontractors.html
[25] https://cnpd.public.lu/en/files-thematics/transfers-international-done-personal.html