Factsheet 7:

Vidéosurveillance

Principle of lawfulness of processing

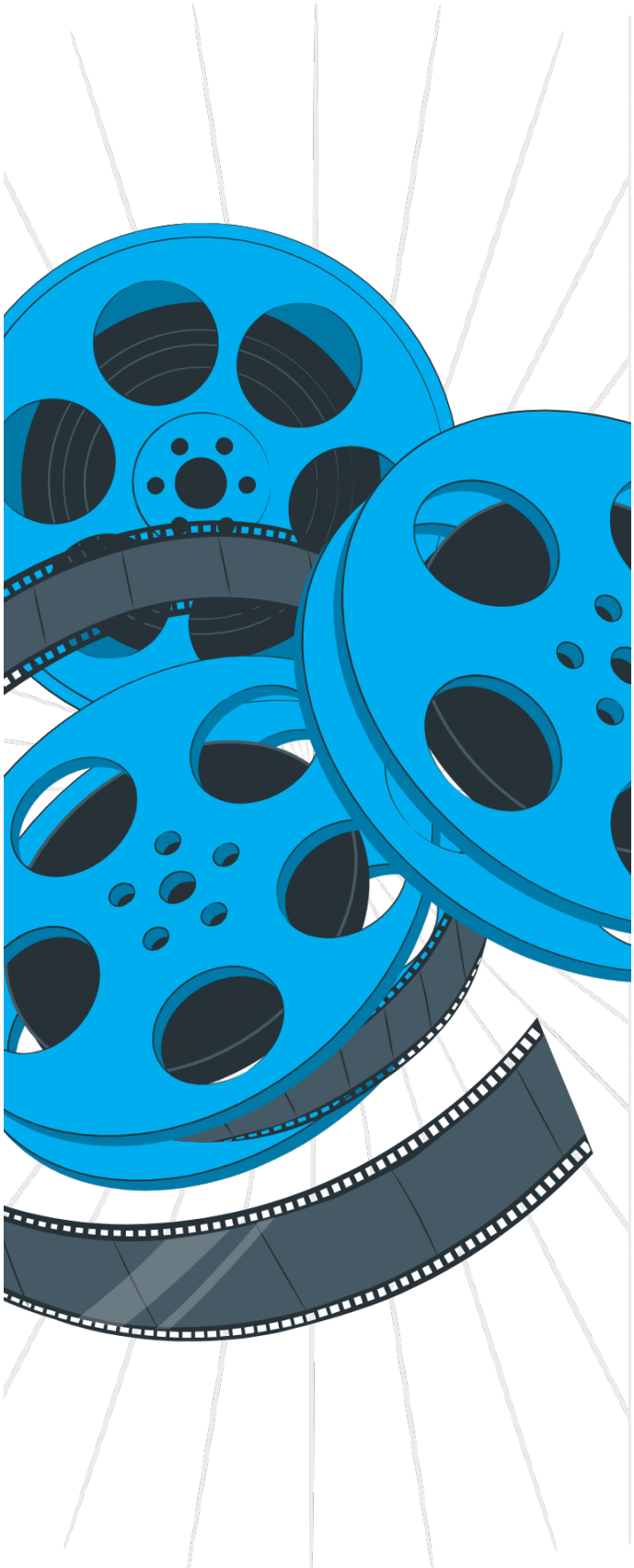
Any processing of personal data must be based on one of the conditions of lawfulness exhaustively listed in Article 6(1) of the GDPR. In the context of a video surveillance system, the most appropriate condition of lawfulness will generally be that of processing necessary for the purposes of the controller's legitimate interests, unless the interests or fundamental rights and freedoms of the person or 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 of the legitimate interest, three cumulative conditions must be met:

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

(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 interests or fundamental rights and freedoms of data subjects must not override the legitimate interests of the controller ('the balancing exercise').

This third condition consists in verifying whether video surveillance is likely to infringe the interests or fundamental rights and freedoms of data subjects, and if so, whether those interests or fundamental rights and freedoms should not override the controller's legitimate interest in implementing a video surveillance system – in which case implementation is not permitted.



Factsheet 7:

Vidéosurveillance

Data minimisation

The principle of necessity implies, first of all, that a controller must only use a video surveillance system where there are no alternative means less intrusive on the privacy of data subjects to achieve the intended purpose. For example, if the controller encounters problems of night-time damage (theft, graffiti, etc.), and wants to remedy them, he must ask himself whether the use of security guards or an 'anti-graffiti' wall covering could not constitute a reasonable solution to achieve the same purpose, while being less intrusive on the privacy of the data subjects.

The principle of data minimisation with regard to 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 this purpose.

Cameras intended to monitor an access point (entrance and exit, threshold, stairway, door, canopy, 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 cover the entire width of any pavement running alongside 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. 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.

Factsheet 7:

Vidéosurveillance

Storage period of images

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 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 storage period must be indicated in the register of processing operations.

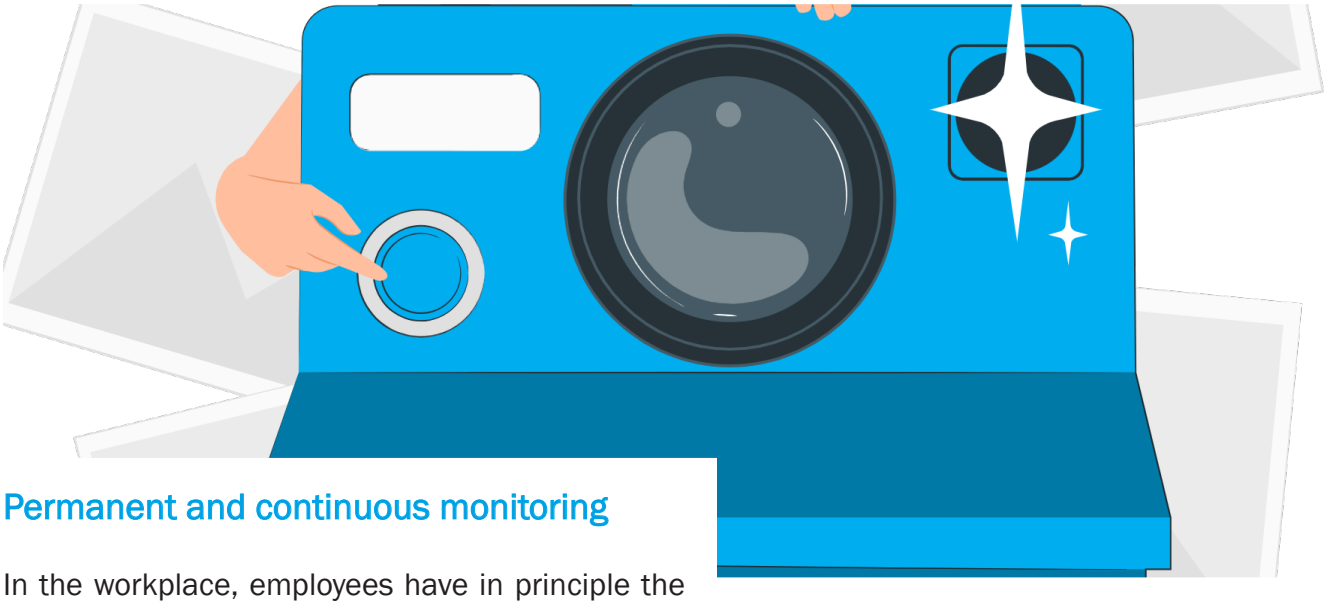
A storage period of more than 30 days is generally considered disproportionate.

In the event of an incident or offence, the images may be retained beyond that period and, where appropriate, communicated to the competent police or judicial authorities.

Finally, the controller must ensure that the images are destroyed after the storage period has expired.

Factsheet 7:

Vidéosurveillance



Permanent and continuous monitoring

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

Compliance with the principle of proportionality means that the employer must use to the means of supervision most protective of the employee's private sphere. Compliance with this principle requires that, for example, automatic and continuous surveillance 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 surveillance 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 on the privacy of employees, the camera will have to be configured

so that employees behind a cash desk are not targeted, by

orienting its field of vision towards the cash register itself and the front of the counter, i.e. the waiting area of customers in front of the counter, in order to enable the identification of perpetrators, for example.

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.

Identité du responsable du traitement :

Coordonnées du responsable du traitement

Finalité(s) poursuivies par la vidéosurveillance :

Information ayant la plus grande influence sur la personne concernée

Plus d'informations concernant cette vidéosurveillance sont disponibles :

Droits des personnes concernées :

Le RGPD vous confère en tant que personne concernée des droits permettant de contrôler l'usage de vos propres données.
Vous disposez notamment d'un droit d'accès et d'un droit à l'effacement.

Pour de plus amples informations sur vos droits, veuillez suivre le

Attention : Ce document constitue un exemple (non contraignant) reprenant les informations du premier niveau. Les différentes rubriques doivent être complétées et adaptées en fonction du système de vidéo-surveillance mis en œuvre par le responsable du traitement.

Update : 4th June 2024