 Procedure No.: PS/00027/2019

938-051119

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and in

based on the following

BACKGROUND

: On 05/22/2018, a claim from A.A.A. against

FIRST

PROVINCIAL COMMISSIONER OF *** LOCATION.1 OF THE NATIONAL POLICE CORPS

for the use of images from the video surveillance system of the Police Station to initiate a

disciplinary procedure, with diversion of the system's own purpose and without there being

been informed that said device could be used for said purpose, in addition

of the lack of proportionality in terms of its use.

The claimant, Inspector of the CNP, is *** POSITION 1 of a group of police officers of the

***BRIGADA.1 of the Police Station of ***LOCALIDAD.1, declares that it performs its functions

rotating shifts and in uniform attached to the Citizen Security Brigade. The night

on ***DATE.1 was on duty and at 11:30 p.m. Inspector ***POST.2 from the

Provincial Citizen Security Brigade, B.B.B. with ***POSITION.1 (head of the

Police station). At that time, the policemen were lending themselves to dinner, the claimant wearing a

black fleece over the uniform, due to the cold in the quarters. Captured

images by the detainee surveillance system of the Police Station in which he appears as

mentioned, the images have been used to instruct him in a disciplinary procedure.

The claimant clarifies that there was no detainee that night, and that the images were

requested by the Inspector ***POSITION.2 on ***DATE.3 to “be able to sanction the

claimant for wearing the uniform incorrectly”, to the official in charge of the

telecommunications that proceeded on ***DATE.2 and that the use thereof for this purpose

is not appropriate, since there were also other officials present who could have

testified about the event.

There is the instruction of the Ministry of the Interior 12/2015 that indicates that in the

detention centers must have a video surveillance system to guarantee the

physical security of persons deprived of liberty and officials who exercise their

custody.

Provides partial copy (crossed out some ends to make it impossible to read

Record of statement given by the Inspector *** POSITION 2,

complete) of:

B.B.B. of

1)

***DATE.3, as "denounced", "proceedings ***PROCEEDINGS.1 in relation to the complaint

of “workplace harassment” requested by the claimant. In said statement, from which it follows that

is related to legal proceedings, the Inspector states that he saw the claimant the

night of ***DATE.1 because he went to deliver the denial of a permit and saw him without the

regulatory uniformity, and admonished him, and in order to prove it, since it was

repeat offender, the next morning he asked the person in charge of telecommunications for a copy of

the images obtained by the cameras near the lobby of his office, to

check whether he had changed his behavior and complied with the order. “However

subsequently caused sick leave, which is why no action has been processed

disciplinary”.

two)

Declaration record (there are also numerous paragraphs crossed out in the document in the

same matter) of the Commissioner, as a witness, stating that the Inspector

POSITION.2 commented on the lack of uniformity of the claimant and the next morning the

The Inspector informed him that he had requested the recording of the cameras in the hall of the

Police Station in order to check if he had finally complied with the order.

3)

Record of the declaration of the person in charge of telecommunications, as a witness, who

indicates that it received the order to obtain a copy of the images of the time slot between 0

hours and 4 hours on *** DATE.2, "knowing later that the object of said

The request was to check if ***POSITION.1 was wearing the regulation uniform”.

Provide a copy of the recording delivery certificate of ***DATE.2 at the request of the

Inspector POST.2

: In view of the facts denounced, by the General Subdirectorate of

SECOND

Data Inspection, the complaint is transferred to the GENERAL DIRECTORATE OF THE POLICE,

to send this Agency the relevant documentation related to the procedures

carried out by the person in charge of treatment, in relation to the facts exposed

in the claim, including in particular the following information:

Detail of the measures adopted by the person in charge to solve the incident and

Clear specification of the causes that have motivated the incidence that has given rise to

1.

gar to the claim.

two.

to avoid the occurrence of new incidents such as the one exposed.

3.

Documentation proving that, in accordance with the provisions of article 12 of the

RGPD, the appropriate measures have been taken to facilitate the exercise of their rights by the affected party.

rights under articles 15 to 22, including a full copy of communications

tions sent in response to requests made.

Four.

informed about the course and outcome of this claim.

Documentation proving that the claimant's right to be

The General Directorate of the Police, dated 08/03/2018 and on the use of

video surveillance cameras of the Provincial Police Station of ***LOCALIDAD.1, states

a)

Attached is the report of the Informatics and Communications Unit of the

Central Logistics and Innovation Headquarters of the General Directorate of the Police. in it

reports that "The management of the CCTV equipment installed in the cells of the

Police station of ***LOCALIDAD.1 is carried out from the police station itself" and continues to give

details of that system.

THIRD: On 09/05/2018, the respondent indicates that he has not received a response by

part of the data protection delegate, and on 12/5/2018 another letter in which he indicates that

He has not received a response from the AEPD.

The same type of writing from the complainant about which he has not received a response has

entry on 02/21/2019 and 03/13/2019.

On 03/04/2019, a letter was sent informing him of the status of his complaint.

FOURTH: On 04/01/2019 it was agreed by the director of the AEPD:

“initiate sanctioning procedure to the Ministry of the Interior-General Directorate of the Police (Provincial Police Station of *** LOCATION.1 of the National Police Corps) for the alleged infringement of article 5.1.b) of the RGPD, infringement typified in article 83.5 a) of the GDPR.

In the shipment made through the nofitic@ platform, it is certified:

“The Support service of the Electronic Notifications Service and Electronic Address Enabled CERTIFIES:

- That the Ministry of Territorial Policy and Public Administration (through the Secretariat General Administration Digital) is currently the owner of the Notification Service Electronic (SNE) and Authorized Electronic Address (DEH) in accordance with the Order PRE/878/2010 and Royal Decree 769/2017, of July 28. The provider of said service since June 26, 2015 it is the National Currency and Stamp Factory-Royal House of the Currency (FNMT-RCM), according to the current Management Assignment of the Ministry of Finance and Public Administrations.

-That the notification was sent through said service:

Reference: 94162555ca5cd5c8ab84 Acting Administration: Spanish Agency for Data Protection (AEPD) Owner: GENERAL DIRECTORATE OF THE POLICE-SERVICES CONTROL UNITS-MIR - S2816015H

Subject: "Notification available in the Folder or DEH of the indicated holder" with the following result:

Availability date: 04/07/2019 05:00:38

Automatic rejection date: 04/15/2019 00:00:00

Automatic rejection generally occurs after ten days have elapsed.

from its availability for access according to paragraph 2, article 43, of

Law 39/2015, of October 1, of the Common Administrative Procedure of the

Public administrations. And in particular, after the term established by the

Administration acting in accordance with the specific legal regulations applicable to

app.

The LPCAP adds in its article 14 "Right and obligation to relate

electronically with the Public Administrations “

2. In any case, they will be obliged to interact through electronic means with the

Public Administrations to carry out any process of a procedure

administrative, at least the following subjects:

a) Legal persons.”

And it is specified in article 41 "General conditions for the practice of

notifications “1. Notifications will preferably be made by means

electronic and, in any case, when the interested party is obliged to receive them by this means.

Notwithstanding the foregoing, the Administrations may make notifications by

non-electronic means in the following cases:

When the notification is made on the occasion of the spontaneous appearance of the

a)

interested party or his representative at the registration assistance offices and request

communication or personal notification at that time.

When, in order to ensure the effectiveness of the administrative action, it is necessary

b)

practice notification by direct delivery of a public employee of the Administration

notifier.

Regardless of the means used, notifications will always be valid.

that allow proof of its sending or making available, of the reception or

access by the interested party or their representative, their dates and times, the full content,

and the true identity of the sender and recipient thereof. The accreditation of the

notification made will be incorporated into the file."

As a consequence, the notification of the agreement is understood to have been produced with all

legal effects.

FIFTH: A copy of instruction 1/2012 of 10/1/2015 is obtained from the website, (numbered

as 12/2015) of the Secretary of State for Security, (SES) approving the

"protocol of action in the areas of custody of detainees of the forces and bodies of

state security". It is incorporated into the file as associated object 2 in the

application that manages it.

In the same figure: 2 f. Video surveillance: The detention centers of the Armed Forces and

State Security Bodies will have video surveillance systems with recording

that contribute to guaranteeing the physical integrity and security of persons deprived of

liberty and that of the police officers exercising their custody. This recording must

be permanently active, regardless of whether the agents in charge of the

custody should maintain permanent control of the cells through the means

of video surveillance.

Video surveillance systems will be governed by the provisions of the Organic Law

4/1997, of 4/08, which regulates the use of video cameras by the Forces and

Security forces in public places. In no case may they allow the

visualization of the toilet areas, in order to preserve the privacy of people

arrested.

A copy of instruction no. 4/2018, signed on 05/14/2018 of

the SES approving the update of the "action protocol in the areas of

custody of detainees of the State Security Forces and Bodies" and is left without

effect instruction 12/2015. It is incorporated into the file as associated object 1 in

the application that manages it.

Figure in point 2.f):

“Video surveillance: The detention centers of the Security Forces and Bodies of the

State will have video surveillance and recording systems that allow viewing

in the light conditions of their cabins, to guarantee the physical integrity and

security of persons deprived of liberty and that of police officers who

exercise their custody.

This recording must be permanently active, regardless of whether

officers in charge of custody should maintain control of the dungeons at

through video surveillance.

The recordings will be kept for thirty days from their capture.

Once this period has expired, they will be destroyed, unless there is an incident in

the course of a detainee's custody or are related to criminal offenses

or administrative serious or very serious in matters of public security; with a

ongoing police investigation or open judicial or administrative proceedings. In

In these cases, the recording will be kept at the disposal of the competent Authorities.”

SIXTH: Within the testing period, the claimant is notified on 06/24/2019 of the start

of the trial period, requesting:

-Sketch of the Police Station of ***LOCATION.1 in which the events took place, in the

to see the situation in which the camera that was used to collect the

image of the claimant and type of room in which the images were collected and selected

images. Color image of the field collected by said camera, identifying the spaces

towards which it focuses.

-Indicate whether it has been delivered to the officials who provide custody services and

custody of detainees on occasion a guide explaining the use or purpose of these

chambers, and if they have been informed that they may be subject to disciplinary action, in what

assumptions, how they have been informed. Specifically the claimant.

-If you know if the claimant has been sanctioned, copy of the resolution, copy of

documents that work in the procedure, and if you are aware of your administrative challenge and

(/or judicial).

-Position/hierarchy held by the person requesting the extraction of the

images, and if the General Directorate of the Police has issued any instructions on the

request for data from video surveillance systems, procedures to follow in the request

of said data, registration of requests, who is responsible for deciding whether they are delivered or not,

or if it deems its preparation convenient.

- If at a disciplinary level, the person who requested the extraction of images can initiate

initiate a disciplinary procedure, procedures that must be carried out.

A copy of the start-up agreement is sent to you so that you can read and

knowledge and with what is requested, contribute what is requested and allege what in your case deem appropriate.

Received the shipment, dated 07/08/2019, the respondent presents a letter in which without responding to what is questioned, provides:

a)

report prepared by the Provincial Commissioner of

***LOCATION.1, subject;

“remitting report on the use of CCTV for disciplinary purposes” signed by the Inspector POSITION.2 Mr. B.B.B., on 01/2/2019. In it he highlights:

-“At 11:30 p.m. last ***DATE.1 appeared in the office of the ***POSITION.1 of the police station…(claimant) checking according to the same The inspector acknowledges in his statement that he was in civilian clothes, two hours after the service had started" he reproached him for the fact and ordered him to to put on the uniform”, “he was aware that the person mentioned was not wearing the uniform during night shifts but lacked evidence” “In anticipation of who failed to comply with the order to render his uniformed service again, requested formally to the person in charge of the CCTV system who would view the images of the night of ***DATE.1 from 11:45 p.m. to check if it had been changed and in Otherwise, extract the precise images to inform the Commissioner of said fact and to be able to prove it”. “The Inspector -claimant- was discharged from ***DATE.4 and then reported him for workplace harassment and for infractions of LO 4/2010 of the regulation of disciplinary regime for infringing the legislation on the use of video cameras. “Both complaints were archived” by the administrative dispatch unit. In the writing it indicates that it is about cameras whose images are obtained and used by the security forces and bodies of the state, and that are governed by the provisions on the matter. Point out the reports

of 2009 numbers 286, 472 of the AEPD on the possibility of using recordings

of the CCTV system installed in police offices as means of evidence

to demand disciplinary responsibilities, it is indicated that "it lacks competences

to assess what evidence may or may not be brought to a disciplinary proceeding”

Indicates that the purpose of the system is the security of the police station and protection

interior and exterior of the building, so I consider that although "they are installed

for this purpose, this does not exclude its use to be able to verify and verify facts object

of an investigation, so it was relevant, legal, justified and proportionate

use it to test and thus be able to purge disciplinary responsibilities if the

there would be”, was limited to some cameras whose purpose is public safety and the

control of entries and exits of citizens, therefore including the hours of

provision of service "

Report number 286/2009 of the Legal Office is associated with the procedure

of the AEPD, signed by the State Attorney on 06/12/2009, found in the SIJ application

that manages said reports, which appears with the following literal:

Entry Ref. 177676/2009 (Trade Union Section S.E.P.-CV of the City Council of

Benidorm)

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/22

Examined your request for a report, sent to this Legal Office, regarding the

query raised by the Trade Union Section S.E.P.-CV of the Benidorm City Council,

please let me know the following:

The consultation raises several questions related to the installation of systems

of video surveillance by the City Council of Benidorm, to check if they comply with the provisions established in the Organic Law 15/1999, of December 13, on the Protection of Character Data.

ter Staff.

The first question asks whether the City Council has obtained authorization from the Spanish Data Protection Agency to install the video surveillance system in the local police building. On this point, it is reported that the Spanish Agency for Data Protection lacks the powers to authorize video surveillance systems.

surveillance, being its competence to ensure that the processing of data derived from the existence of such systems is in accordance with the provisions of Organic Law 15/1999, of December 13, Protection of Personal Data, and Instruction 1/2006, of November 8 of this Agency.

However, we can point out that the aforementioned City Council notified and has registered in the General Registry of Data Protection, a file of video surveillance cameras of the Police, whose name and declared purpose is "Access control and surveillance of the Police building" and "video surveillance".

In the declaration of the aforementioned file, it is stated that the General Provision of creation of the file was published in the Bulletin of the Province, with the number 00067 and date of April 9, 2008.

Regarding the period of conservation of the images, taking into account the purpose described in the Provision for creating the file, the Instruction 1/2006, of November 8, of the Spanish Agency for Data Protection, on the treatment processing of personal data for video surveillance purposes through camera systems or video cameras where article 6 provides that "The data will be canceled in the maximum period of one month from its capture."

Regarding the term that the images can be kept, the Agency has ruled mentioned in the report of July 3, 2008, regarding the foundation of said period, indicating

what

“Article 6 of instruction 1/2006, which regulates the term of conservation of

images is closely related to the provisions of article 4.5 of the

Organic Law 15/1999 that states the following "The data will be canceled when

have ceased to be necessary or relevant for the purpose for which they were intended.

collected or registered.”, said provision is reiterated in article 8.6 of the Re-

development regulation of the Organic Law. The Agency's criteria based on

said principle has been to understand that the images recorded to comply with the fi-

security purpose must be kept for a maximum of one month, one

Once this purpose has been fulfilled, they must be cancelled. Therefore, said term

remains in force after the entry into force of the Regulation since it does not oppose the

provisions contained therein.

Furthermore, it is necessary to point out that the term of one month that in

the Instruction is set to cancel the images, it is not arbitrary, since

It has been decided to follow the same criteria as that established in Organic Law 4/1997,

of August 4, which regulates the use of video cameras by the Armed Forces

and State Security Corps in public places, which in its article 8 points out

which “The recordings will be destroyed within a maximum period of one month from their

catchment".

On the other hand, the instruction expressly states in article 6 that “the

data will be canceled within a maximum period of one month from its collection”, wants

This means that once this period has elapsed, the images must be

celadas, which implies the blocking of the same as it is established, the Or-

15/1999 that in article 16.3 states that "the cancellation will give rise to blocking

storage of the data, keeping it only at the disposal of the Administrations

Public authorities, Judges and Courts, for the attention of the possible responsibilities

des born of the treatment, during the term of prescription of these. Completed on

said period must proceed to the deletion.

The query also raises whether the omission of the duty to inform of the rights of

access, rectification, cancellation and opposition of the data makes the cameras illegal

flush In order for the installation of these cameras to comply with the provisions of the

data protection, compliance with certain requirements such as; the le-

quality of image processing. Article 6.1 of Organic Law 15/1999 to which

article 2 of Instruction 1/2006, establishes that "The treatment of data of

personal character will require the consent of the affected party, unless the Law provides otherwise.

stuff". What forces to resort to a Law that provides for the treatment of images without

bar the consent of the affected party.

In this sense, the Organic Law 2/1986, of March 13, of Forces and Corps of

Security in its article 11, regulates its functions stating that “1. The Forces and Bodies

The State Security post has the mission of protecting the free exercise of human rights.

and freedoms and guarantee citizen security through the performance of the following

functions: (...) c) Monitor and protect public buildings and facilities that require it”,

Consequently, we can conclude that Organic Law 2/1986 legitimizes the treatment of

the images you collect at police stations.

Likewise, the duty to inform must be complied with in accordance with the provisions of the

article 3 of Instruction 1/2006, and notify and register the file in the General Registry of

Data Protection. In addition to allowing the exercise of the rights referred to

articles 15 and following of Organic Law 15/1999, under the terms of article 5 of
The instruction. In the exercise of rights, specialties must be taken into account.
from article 23 of the Organic Law 15/1999, since the exceptions to the
rights of access, rectification and cancellation in the files for which it is responsible
the State Security Forces and Bodies.
Finally, it is considered if the recordings obtained through the video system
installed in the local police offices, they can be used as me-
god of evidence to demand disciplinary responsibilities from the police. On this point,
It should be noted that the Agency lacks the powers to assess what evidence or not
may be brought in a disciplinary proceeding.

However, according to the purpose declared in the General Registry of Protection of
Data, the file created is to control and monitor access to the building, therefore, if the res-
disciplinary responsibilities, were derived from access to it (entry time and
exit by the police) they could be used, not being able to be used for
other types of purposes, which are not declared.
Lastly, in the event that the consultant considers the existence of a
action allegedly contrary to Organic Law 15/1999, you must address your complaint
before this same body, with the purpose of adopting the necessary measures to
in order to verify whether or not the opening of the corresponding sanctioning file proceeds
being so that article 37.1.g) of the Law attributes to this Agency the power to sanction-
ra in terms of data protection.

In any case, the allegations made by the complainant should contain the

supporting documentation of the actual reality of the facts. Said complaint must

be submitted in writing and address the Spanish Agency for Data Protection in the terms

ments established in article 70 of the Law on the Legal Regime of Public Administrations

Public and common Administrative Procedure, must contain:

a)

b)

c)

d)

Name and surnames of the interested party and, where appropriate, of the person who represents him,

as well as the identification of the preferred means or the place that is indicated for

of notifications.

Facts, reasons and request in which the request is specified clearly.

Place and date.

Signature of the applicant or accreditation of the authenticity of his will expressed by

any medium.

Body, center or administrative unit to which it is addressed. (in your case it would be the sub-

and)

General Directorate of Data Inspection of this Agency"

Report 472/2009 of the State Attorney, of

10/20/2009:

Entry Ref. ***REFERENCE.1 (Foundation ***FOUNDATION.1)

"Having examined your request for a report, sent to this Legal Office, regarding the

query raised by the ***FUNDACIÓN.1, please inform you of the following:

The consultation raises several issues related to the issues of

video surveillance, to adapt its performance to both the Organic Law 15/1999, of 13

December, on the Protection of Personal Data, as well as the Regulation of

development of the same and the Instruction 1/2006, of November 8, on the treatment

of personal data for surveillance purposes through camera systems or

camcorders.

The first question refers to the obligation to keep the images blocked,

In this regard, it should be noted that the period of conservation of the images, according to the

Article 6 of Instruction 1/2008 that “The data will be canceled within the maximum period

one month from the time it was picked up.

Regarding the term that the images can be kept, the Agency has ruled

mentioned in the report of July 3, 2008, regarding the foundation of said period, indicating

what

“Article 6 of instruction 1/2006, which regulates the term of conservation of

images is closely related to the provisions of article 4.5 of the

Organic Law 15/1999 that states the following "The data will be canceled when

have ceased to be necessary or relevant for the purpose for which they were intended.

collected or registered.”, said provision is reiterated in article 8.6 of the Re-

development regulation of the Organic Law. The Agency's criteria based on

said principle has been to understand that the images recorded to comply with the fi-

security purpose must be kept for a maximum of one month, one

Once this purpose has been fulfilled, they must be cancelled. Therefore, said term

remains in force after the entry into force of the Regulation since it does not oppose the

provisions contained therein.

Furthermore, it is necessary to point out that the term of one month that in the Instruction is set to cancel the images, it is not arbitrary, since It has been decided to follow the same criteria as that established in Organic Law 4/1997, of August 4, which regulates the use of video cameras by the Armed Forces and State Security Corps in public places, which in its article 8 points out which “The recordings will be destroyed within a maximum period of one month from their catchment".

On the other hand, the instruction expressly states in article 6 that “the data will be canceled within a maximum period of one month from its collection”, wants This means that once this period has elapsed, the images must be canceled, which implies the blocking of the same as it is established, the Law Organic 15/1999 that in article 16.3 states that "the cancellation will give rise to the blocking of the data, keeping it only available to the Public Administrations, Judges and Courts, for the attention of possible responsibilities arising from the treatment, during the prescription period of these. Once the aforementioned period has expired, the deletion must proceed.

On the other hand, the Development Regulation of the LOPD, approved by Royal Decree 1720/2007, of December 21, defines in its article 5.1. b) cancellation as “Procedure by virtue of which the person in charge ceases to use the data. The cancellation will imply the blocking of the data, consisting of the identification and reservation of the same in order to prevent their treatment except for making them available to Public Administrations, Judges and Courts, for the attention of possible responsibilities arising from the treatment and only during the prescription period of these responsibilities. Once this period has elapsed, the suppression of the data."

Regarding the way to carry out the blockade, it was pointed out in this report

Agency of June 5, 2007 that "must be carried out in such a way that it is not possible to

access to the data by staff who routinely had such access, for example

example, the personnel who provide their services in the consulting center, limiting access to

a person with the maximum responsibility and by virtue of the existence of a requirement

judicial or administrative act to that effect. In this way, despite continuing the treatment of

the data, access to them would be entirely restricted to the people to whom

which has been referenced."

As for the period of conservation of the blocked images, we can only

reiterate what was stated in the report attached by the consulting entity of 18

February 2009 in which it is stated "it is impossible to establish a taxative enumeration

of the same, fundamentally having to take into account, as already indicated,

previously, the prescription periods of the actions that could derive from

the legal relationship that links the consultant with his client, as well as those derived from the

tax regulations or the limitation period of three years, provided for in article 47.1 of

the Organic Law 15/1999 itself in relation to the behaviors constituting infringement

very serious."

And as for the last question raised, it is necessary to distinguish whether the regime of

recordings is made in digital format or not, because in the event that it is made in

digital port, there is an automated data processing, which implies the obligation to

comply with the basic level security measures provided for in article 94 of the Regulations.

development of the Organic Law 15/1999.”

b) Copy of the Report of the

Subdirectorate General of Logistics and Innovation of

3/12/2018, recipient “data protection delegate. Technical Office”

It now speaks of the "video surveillance" file for the purpose of

“guarantee the interior and exterior protection of the CNP Commissioners and the buildings,

facilities and centers supervised by the same, Its use is aimed at the "security and

protection". The system is regulated by Internal Order 1865 of 11/30/2016 of the Ministry of

Interior by which the Order INT/1202/2011, of 4/05, which regulates the

personal data files of the Ministry of the Interior, BOE 12/12/2016. In the

single article indicates that both the new creation of the files that are contained as

the modification is governed by the LOPD and development regulations.

The file is created in it: "Video surveillance" of which the following stand out:

a.2) Purpose: Guarantee the internal and external security and protection of the Police Stations

of the National Police Corps and of the buildings, installations and centers supervised by the

same.

a.3) Intended uses: Security and protection.

b) Origin of the data:

b.1) Collective: People who are in video-monitored areas of Police Stations

of the National Police Corps or of the buildings, installations and centers supervised by the

same.

b.2) Origin and collection procedure: Closed circuit television.

c) Basic file structure:

c.1) Description of the data:

Identification data: Image/voice.

c.2) Treatment system: Automated.

d) Planned data communications: judicial bodies, Public Prosecutor's Office and other ser-

vices of the National Police Corps for the exercise of legally entrusted functions.

as well as to other Security Forces and Bodies for the exercise of their functions.

protection of public security, in accordance with the provisions of article 22.2

of Organic Law 15/1999, of December 13, in compliance with the principles of collaboration

cooperation, mutual aid and reciprocal cooperation and information established by the Organic Law

nica 2/1986, of March 13.

e) Planned international data transfers to third countries: Not planned.

f) Body responsible for the file: Subdirectorate General for Logistics, calle Julián Gon-

zález Segador, no number, 28043 Madrid.

g) Service or Unit before which the rights of access, rectification,

tion, cancellation and opposition: General Secretariat of the Subdirectorate General for Logistics,

Julián González Segador street, no number, 28043 Madrid.

i) Basic, medium or high level of security that is required: High.

He adds that "Currently the telecommunications area of the

IT and communications has a procedure for the treatment of

video surveillance images where the following aspects are determined: "The security system

access control to the images, they consist of an alphanumeric key with two categories

of users: administrator with permissions to view and extract images and

Basic user with viewing permissions only. ICT delegates have the permits

of user administration and therefore for the extraction of images in all the

provincial commissioners of the CNP”

SEVENTH: On 09/18/2019, a response was given to the claimant's letter requesting

inform you of the status of the procedure, ask to be considered interested in it,

deciding to inform you of the end of the procedure for the purpose of consulting the website of the

resolution.

EIGHTH: On 11/18/2019, a resolution proposal was issued with the literal:

“That by the Director of the Spanish Agency for Data Protection, the

with a warning to the GENERAL DIRECTORATE OF THE POLICE (MINISTRY OF THE

INTERIOR), for an infringement of Article 5. 1 b) of the RGPD, typified in Article 83.5

of the GDPR.”

The respondent presents allegations indicating that the events occurred before

the entry into force of the RGPD, and this is important because "During the period of validity of

the previous LOPD the Courts have maintained that the use of images from the

Police station cameras to check the correct functioning of the services

police cannot be considered an incompatible purpose prohibited by law, although

Its main use is the security of goods and people.

PROVEN FACTS

The Inspector ***PUESTO.2 of the Provincial Citizen Security Brigade of the

1)

commissioner of ***LOCALIDAD.1, Mr. B.B.B., observed on the night of ***DATE.1 that the

claimant, CNP Inspector and ***POST.1, is not properly uniformed, wearing

a black fleece jacket according to the claimant, being reprimanded by him and ordered to

properly uniformed, according to Inspector ***POSITION.2, leaving the

place. The next day, the Inspector ***POST.2, decides to verify if the claimant complied

your order and request a copy of the images from the cameras between 0 and 4 a.m.

***DATE.2. The extraction of the images is produced by personnel dedicated to

telecommunications in the same police station of ***LOCALIDAD.1, personnel who stated,

that no motive was contained or explained, knowing later that the object

of said request was to check if ***POSITION.1 was wearing the regulation uniform". Nope

there is a written request, if any, to extract the images, and it is provided

copy of record delivery record of ***DATE.2, at the request of the Inspector

***POSITION.2

According to the claimant, on the night of ***DATE.1 there were no detainees

two)

in the comisary.

The Commissioner of the CNP of

***LOCATION.1 in which the

3)

claimant, has video surveillance cameras for the detainees' cells. I know

This recruitment is governed by the action protocol in the Detainee Custody Areas

of the State Security Forces and Bodies, instruction of the Secretary of State

of Security 4/2018, signed on 05/14/2018 and that leaves without effect the Instruction number

12/2015 of the Secretary of State for Security. It appears as an object that of "establishing

the rules of action of the personnel in charge of the custody of detainees … with the purpose of

to guarantee the rights of detainees and their safety and security

police."

"The recordings will be kept for thirty days from their capture. One time

At the end of this period they will be destroyed, unless there is an incident in the

course of custody of a detainee or are related to criminal offenses or

serious or very serious administrative offenses in matters of public security; with a

ongoing police investigation or open judicial or administrative proceedings. In

In these cases, the recording will be kept at the disposal of the competent Authorities."

Unlike the previous instruction, this one does not indicate that the

video surveillance will be governed by the provisions of Organic Law 4/1997, of 4/08, by which

the use of video cameras by the Security Forces and Bodies in

public places.

In the testing period, it is also indicated by the Commissioner of

4)

*** LOCATION.1 that has cameras for the security of the police station and protection

interior and exterior of the building and in the Report of the General Subdirectorate of Logistics and

Innovation of 3/12/2018, addressee "data protection delegate. Technical Office"

It is specified that these cameras are for the "purpose of" guaranteeing the interior protection and

exterior of the CNP Police Stations and of the buildings, installations and centers guarded by

the same. Its use is aimed at "safety and protection". To this system is applied the

LOPD, in accordance with the file creation order- Order INT/1202/2011, of 4/05,

by which the personal data files of the Ministry of the Interior are regulated,

BOE 12/12/2016

5)

The respondent has not specified, by not responding in evidence, with what type of

camera the images were obtained on the fulfillment of the uniformity by the

claimant, in what spaces were taken, to which of the two systems corresponds

(surveillance of cells or of the police station in general) and what protocol exists for requesting

pictures and delivery.

6)

None of the purposes of the data collection treatment of the two systems,

of video surveillance contemplate the use of their images for the purpose of verification of

behaviors, compliance with the internal regime, or disciplinary offenses that could

commit the agents, which was the purpose of the petition and extraction of those of the claimant the

night of ***DATE.2.

7)

In addition, it is accredited that the image request and its delivery to the Inspector

***POSITION.2, superior of the claimant is not, nor does it appear in any protocol that regulates the

issue, and only authorized persons must have access to the images.

expressly in some type of document or protocol that regulates the request for images,

reasons and documentation of those aspects.

8)

There is no evidence that disciplinary proceedings have been initiated or resolved against the

claimant or based on the lack of uniformity on the night of ***DATE.1, although if the

request of the images and their delivery.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of Regulation (EU) 2016/679 of the

European Parliament and of the Council of 04/27/2016 on the protection of people

physical with regard to the processing of personal data and the free movement of

your data (hereinafter GDPR); recognizes each control authority, and as established established in art. 47 of Organic Law 3/2018, of 5/12, on the Protection of Personal Data- them and guarantee of digital rights (hereinafter LOPDGDD), the director of the AEPD is competent to initiate and resolve this procedure.

II

In the present case, given the lack of specification of the claim, by not specifying with what type of camera or its location or regime are the images communicated by the claimant, it can be deduced that there could be two types of cameras in the Police Station where the events take place. The result is that whatever the system of cameras employed, the extraction for the reasons that occurred and directly by the first superior of the claimant, violates the RGPD in that it is not contemplated in neither of the two systems the use of reprimand of irregular behaviors by the Agents, and also does not appear regulated in your case who has to request the images.

On the one hand, the cameras that monitor the cells of the detainees, with their of the Organic Law ***LAW.1 which regulates the use of video cameras by the Security Forces and Bodies in public places, requires an authorization prior issuance of a report by a collegiate body, and the "resolution by which agrees the authorization must be motivated and referred in each case to the public place concrete to be observed by the video cameras. Said resolution It will also contain all the necessary limitations or conditions of use, in particular the prohibition of taking sounds, except when there is a specific and precise risk, as well

such as those referring to the qualification of the persons in charge of the exploitation of the system for processing images and sounds and the measures to be adopted to guarantee the compliance with current legal provisions. Likewise, you must specify generically the physical environment that can be recorded, the type of camera, its technical specifications and the duration of the authorization, which will be valid for a maximum of one year, after which term, its renewal must be requested."

The following are indicated as authorization criteria to take into account:

"To authorize the installation of video cameras will be taken into account, in accordance with the principle of proportionality, the following criteria: ensure the protection of buildings and public facilities and their accesses; safeguard useful facilities for the national defense; verify violations of citizen security, and prevent the causation of damage to persons and property." Article 4

Article 6 outlines the "principles of use of video cameras:

1. The use of video cameras will be governed by the principle of proportionality, in its double version of suitability and minimal intervention.
2. The suitability determines that the camcorder may only be used when it is adequate, in a specific situation, for the maintenance of citizen security, of in accordance with the provisions of this Law.
3. The minimum intervention requires weighing, in each case, between the purpose intended and the possible affectation by the use of the video camera to the right to honor, to the image itself and the intimacy of people.
4. The use of video cameras will require the existence of a reasonable risk for the

citizen security, in the case of fixed ones, or of a specific danger, in the case of

mobiles.

5. Video cameras may not be used to take images or sounds from inside the

the dwellings, nor of their lobbies, except with the consent of the owner or judicial authorization, nor

of the places included in article 1 of this Law when it is affected directly and

serious to the intimacy of people, nor to record conversations of

strictly private nature. The images and sounds obtained accidentally in

These cases must be destroyed immediately, by whoever is responsible for

its custody.

The space that these cameras have to focus on is related to the

mandatory existence of video surveillance cameras to observe and guarantee the

safety of detainees in police cells. This modality related to the

public safety does not seem directly related to the lack of uniformity of the

claimant public employee, who states, being the night of ***DATE.1 that before the

intense cold that exists in said Police Station, he wore a fleece over his uniform.

Therefore, by reason of the matter, nor those whose purpose is the surveillance of

detainees in cells, nor those installed in the police station, to which is applied

the LOPD, since May 2018 the RGPD, are likely to be used for the purpose of

that they have been, without having been previously informed of said purpose. To do this, you should first

having decided by the person responsible for the treatment, that the follow-up of the eventual

behaviors that can be disciplined through said means and modality of

video surveillance for the agents in the police station was undertaken with these means, an issue

that affects their labor rights and their privacy and proportionality should be assessed

and suitability of the system, or for what assumptions.

Instruction 1/201/2006, of 8/11 of the Spanish Agency for the Protection of

Data, on the processing of personal data for surveillance purposes through

camera or video camera systems, BOE 12/12 indicated in its preamble:

In connection with the installation of video camera systems, it will be necessary

weigh the legal rights protected. Therefore, all installations must respect the

principle of proportionality, which ultimately means, whenever possible,

adopt other less intrusive means to the privacy of people, in order to

prevent unwarranted interference with fundamental rights and freedoms.

In view of the lack of clarification by the complainant of the type of cameras with which

obtained the images, nothing contributed to what was requested in tests, it should be indicated that the use

of cameras or video cameras should not be the initial means to carry out functions

so that, from an objective point of view, the use of these systems

it must be proportional to the aim pursued, which in any case must be legitimate.

Regarding proportionality, despite being an indeterminate legal concept, the

Ruling of the Constitutional Court 207/1996 determines that it is "a requirement

common and constant for the constitutionality of any restrictive measure of rights

fundamental, among them those that suppose an interference in the rights to the integrity

physical and privacy, and more particularly of the restrictive measures of rights

principles adopted in the course of criminal proceedings is determined by the

strict observance of the principle of proportionality'.

Its article 4 indicates:

1. In accordance with article 4 of Organic Law 15/1999 of December 13, of

Protection of Personal Data, the images will only be treated when they are

adequate, relevant and not excessive in relation to the scope and purposes

determined, legitimate and explicit, that have justified the installation of the cameras or

camcorders."

Article 1 of the RGPD points out "This Regulation establishes the rules

relating to the protection of natural persons with regard to the treatment of

personal data and the rules relating to the free movement of such data.

2. This Regulation protects the fundamental rights and freedoms of

natural persons and, in particular, their right to the protection of personal data."

The art. 4.1 and . 2 of the RGPD indicates "1) "personal data": all information about a

identified or identifiable natural person ("the interested party"); will be considered a natural person

identifiable person any person whose identity can be determined, directly or indirectly, in

by an identifier, such as a name, phone number,

identification, location data, an online identifier, or one or more elements

inherent to the physical, physiological, genetic, mental, economic, cultural or social identity of

said person;

2) "processing": any operation or set of operations performed on data

personal information or sets of personal data, whether by automated procedures or

no, such as the collection, registration, organization, structuring, conservation, adaptation or

modification, extraction, consultation, use, communication by transmission, diffusion or

any other form of authorization of access, collation or interconnection, limitation, suppression

or destruction;

The video surveillance system in this case supposes an identification

directly from the person whose actions are collected when they are in your recording space.

In this case, the Commissioner had two different systems implemented:

video surveillance for the cells of detainees and the general for security of the

facilities, being the purpose different, otherwise none of them for the purpose

verification of behavior or repression of infractions of the agents.

In this case, personal data are considered to be the appearance of the Agent,

identifiable, along with his clothing, relating whether the claimant had appropriated the

same clothing to the internal staff regulations, capturing as accreditation

irrefutable the obtaining of the images that focused that space between a section

differentiated schedule, which was selected by ***POSITION.2, which hours before had

seen and warned of the lack of uniformity, in order to sanction a fault.

The use of images in both systems, recording, conservation, extraction,

It is related to the safety of people, agents or facilities. However, in

In this case, they have been used in the workplace as a means of verification. The AEPD does not

pronounces on the validity of the images that will be provided to the procedure

disciplinary, but by the legitimacy and legality of the same in accordance with the regulations of

data protection and the treatment that is accredited is carried out with the data

personal of the affected.

Article 18.4 of the Spanish Constitution indicates: “the law will limit the use of the

information technology to guarantee the honor and personal and family privacy of citizens and the

full exercise of their rights.

In accordance with the ruling of the Constitutional Court 254/1993 that initiates the

doctrine of the right to data protection: “…From all that has been said, it turns out that the content

of the fundamental right to data protection consists of a power of disposition and control over personal data that empowers the person to decide which of those data to provide to a third party, be it the State or an individual, or what this third party can collect, and that also allows the individual to know who owns that personal data and for what, being able to oppose that possession or use. These powers of disposition and control on personal data, which constitute part of the content of the fundamental right to data protection are legally specified in the power to consent to the collection, Obtaining and accessing personal data, their subsequent storage and treatment, as well as its use or possible uses, by a third party, be it the State or an individual. And that right to consent to the knowledge and treatment, computerized or not, of the data personal, requires as essential complements, on the one hand, the faculty of knowing at all times who has these personal data and to what use they are submitting, and, on the other hand, the power to oppose that possession and uses."

As a conclusion of the two reports of the Legal Office of the AEPD alleged by the claimed, it cannot be inferred that the video surveillance cameras for internal control located in the Police Stations, whether they are ticket control, or of another type, which is not referred to the reports refer, insofar as their purpose is the security of their facilities and their personal, there is no extensive use for the purpose of correcting disciplinary behaviors of its employees, whether they are police officers, or other types of personnel, such as control of the claimant's uniform. With such data processing for that disciplinary purpose, it is affected ta to the legal sphere of its staff, creating a means of verifying compliance conduct without prior information that affects a fundamental right, without security any legal entity in terms of its use, subjects authorized for the request, exaction, and derights of the affected party of access, cancellation, conservation and non-manipulation, security, etc.

Nor is it true that the LOPD enabled uses other than the intended purpose.

pia of the file or treatment. In addition, it is recalled that incompatible use is not sanctioned,

but a use for a purpose for which it was not reported, alien to the expectations of the

employees.

III

The RGPD, article 5.1.b) of the RGPD indicates:

"1. The personal data will be:

b) collected for specific, explicit and legitimate purposes, and will not be processed

subsequently in a manner incompatible with those purposes; according to article 89,

section 1, further processing of personal data for archiving purposes in the interest

public, scientific and historical research purposes or statistical purposes shall not be considered

incompatible with the original purposes ("purpose limitation")

Requirement for data processing to be in accordance with the provisions of the

regulation is that it is legitimized in the provisions of its article 6 and that it

adjustment to its principles of article 5. However, it is not possible to legitimize the processing of data

of video surveillance for purposes of verifying compliance with the internal regulations in the

employee consent. For this, it will be necessary to go to another legitimate base that

could be the control of compliance with established legal obligations, but as

previously pointed out, this would require assessing various elements and taking into account

various aspects, among others the proportionality of use, in this case of an order that

It occurred when he saw the Agent who was not properly uniformed, so that he would do it.

In this case, the images are treated with a purpose that is not the one foreseen by the

treatment operations established by the video surveillance systems of the

Police station.

The LOPD is applied, or the RGPD is applied, the basic principle breached, in case of

that the system was considered proportional to the ends and had been implemented, is that it

those affected, in this case the claimant, were informed of the use of the system, their

consequences and the rights that derive from it. The circumstance of not

having been done supposes, with its use, a diversion of purpose, since the system was

contemplated for security purposes of the Commissioner, the Agents, or where appropriate, the

arrested. The unfulfilled principle is the one that opens the infraction to the one claimed, 5.1 b)

of the GDPR.

On the other hand, the consequences in both regulations is the declaration of infraction

LOPD or the warning, RGPD. In both cases it supposes the declaration of a form of

act not in accordance with the data protection regulations and the requirement to

adequacy of conduct in the future, if it has not been done during the substantiation of the

same as what the standard provides.

In this sense, it is unknown if the system of

video surveillance in some case similar to the one denounced in said police station, given the lack

of explanations as requested in tests.

IV

In addition, for the virtuality of the system's operation, it would be necessary to

compliance with the principle, which imposes the obligation of prior information on employees

and consultation with their representatives. In this sense, it is worth mentioning the judgment

of the Constitutional Court of 29/2013 of 11/02 that in a case of control by

video surveillance of an employee of the University of Seville who was suspected of being

Irregularities in the fulfillment of their working day, in its legal basis VII

indicated:

“This right to information also operates when there is legal authorization to

collect the data without the need for consent, since it is clear that one thing is the

need or not for authorization of the affected and another, different, the duty to inform him about

its holder and the purpose of the treatment. It is true that this informative demand does not

can be taken as absolute, since it is possible to conceive limitations for reasons

constitutionally admissible and legally provided for, but it should not be forgotten that the

Constitution has wanted the Law, and only the Law, to be able to set the limits to a right

fundamental, also demanding that the cut they experience is necessary to achieve

the legitimate intended purpose, proportionate to achieve it and, in any case, respectful of the

essential content of the restricted fundamental right (SSTC 57/1994, of February 28

[RTC 1994, 57], F. 6; 18/1999, of February 22 [RTC 1999, 18] , F. 2, and in relation to the

right to personal data protection, STC 292/2000 [RTC 2000, 292], FF. 11 and

16).”

There is no express legal authorization for this omission of the right to

information on the processing of personal data in the field of relationships

employment, without the interest in controlling the activity being sufficient as a basis for this purpose, and

without it being sufficient that, in the specific case, that data processing is

possibly proportionate to the end pursued.

The TCo, 29/2013 added that “prior and express information,

precise, clear and unequivocal to the workers of the purpose of controlling the activity

to which this recruitment could be directed" and that "it should specify the

characteristics and scope of the data processing that was going to be carried out, that is, in what cases the recordings could be examined, for how long and with what purposes, specifying very particularly that they could be used for the imposition of disciplinary sanctions for breaches of the employment contract.

The idea from which one must start when determining the essential content of the right that enshrined in article 18.4 of the CE is that if the legislation recognizes certain guarantees linked to the fundamental right to the protection of personal data, in this case, the previous informative duty must be respected that allows to have full knowledge of who owns the personal data and what it is used for. Only then can the worker or employee know about the use and consequences of the collection of their data, "informative self-determination", and also request, as part of their right, the limitation, access, cancellation or deletion of data.

In this case, the concrete and punctual extraction, predetermined of a strip time in which the claimant was not in uniform, has served directly to control compliance with its uniformity with a video surveillance system that did not have that purpose.

v

Article 58.2 b) and d) of the RGPD provides the following: "Each supervisory authority shall have all of the following corrective powers listed below:

b) sanction any person responsible or in charge of the treatment with a warning when the treatment operations have violated the provisions of this Regulation; -

d) order the person in charge or in charge of the treatment that the operations of treatment comply with the provisions of this Regulation, where appropriate, in accordance with a certain way and within a specified period;

The imposition of this measure is compatible with the sanction of warning,

according to the provisions of art. 83.2 of the GDPR.

No specific measures are imposed to be implemented by the respondent, since there is no

the treatment is detailed with the purpose for which it has been carried out, and must

not be used again on another occasion, unless it proves the proportionality of the

purpose of the use of verification of the disciplinary regulation and the adequate and clear

information on said use to those affected. As stated in this resolution,

a new purpose would have to be added if it decided to carry out disciplinary control

by the video camera capture system inside the police stations, for which

should meet the requirements of the GDPR.

Article 83.5.a) of the RGPD indicates

"5. Violations of the following provisions will be sanctioned, in accordance with

section 2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of

of a company, of an amount equivalent to a maximum of 4% of the turnover

global annual total of the previous financial year, choosing the highest amount:

a) the basic principles for the treatment, including the conditions for the

consent under articles 5, 6, 7 and 9;"

Article 83.7 of the RGPD indicates:

"Without prejudice to the corrective powers of the control authorities under the

Article 58(2), each Member State may lay down rules on whether it can,

and to what extent, impose administrative fines on authorities and public bodies

established in that Member State.

The LOPDGDD, in its article 77 indicates

The Spanish legal system has chosen not to sanction with a fine those

public entities, as indicated in article 77.1. c) and 2. 4. 5. and 6. of the

LOPDDG: “1. The regime established in this article will be applicable to

treatments for which they are responsible or in charge:

c) The General Administration of the State, the Administrations of the communities

autonomous and the entities that make up the Local Administration.

2. When those responsible or in charge listed in section 1 committed

any of the infractions referred to in articles 72 to 74 of this organic law,

the data protection authority that is competent will issue a resolution sanctioning

to them with warning. The resolution will also establish the measures that

appropriate to adopt so that the conduct ceases or the effects of the infraction are corrected.

would have committed

The resolution will be notified to the person in charge or in charge of the treatment, to the body of which

depends hierarchically, where appropriate, and those affected who had the status of

interested, if any.

4. The data protection authority must be notified of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

5. They will be communicated to the Ombudsman or, where appropriate, to the analogous institutions of

the autonomous communities the actions carried out and the resolutions issued to the

protection of this article.

6. When the competent authority is the Spanish Data Protection Agency,

this will publish on its website with due separation the resolutions referring to the

entities of section 1 of this article, with express indication of the identity of the

responsible or in charge of the treatment that had committed the infraction."

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE a sanction of WARNING to the GENERAL DIRECTORATE OF

THE POLICE (MINISTRY OF THE INTERIOR), with NIF S2816015H, for an infraction of the

Article 5.1 b) of the RGPD, in accordance with Article 83.5 and 58.2.b) of the RGPD.

/

SECOND: NOTIFY this resolution to the GENERAL DIRECTORATE OF THE

POLICE (MINISTRY OF THE INTERIOR).

THIRD

in accordance with the provisions of article 77.5 of the LOPDGDD.

: COMMUNICATE this resolution to the OMBUDSMAN, of

FOURTH: Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6

of the LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the Director of

the Spanish Agency for Data Protection within a period of one month from the day

following the notification of this resolution or directly contentious appeal

before the Contentious-Administrative Chamber of the National High Court, with

in accordance with the provisions of article 25 and section 5 of the fourth additional provision

of Law 29/1998, of 13/07, regulating the Contentious-administrative Jurisdiction, in

within two months from the day following the notification of this act, as

the provisions of article 46.1 of the aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP,

the firm decision may be provisionally suspended in administrative proceedings if the interested party states its intention to file a contentious-administrative appeal. If this is the
In this case, the interested party must formally communicate this fact in writing addressed to the Spanish Agency for Data Protection, presenting it through the Registry Electronic Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other records provided for in art. 16.4 of the aforementioned Law 39/2015, of 1/10.
You must also transfer to the Agency the documentation that proves the filing effectiveness of the contentious-administrative appeal. If the Agency were not aware of the filing of the contentious-administrative appeal within two months from the day following the notification of this resolution, it would end the suspension precautionary

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es