

Procedure No.: PS/00051/2019

938-0419

## RESOLUTION OF SANCTIONING PROCEDURE

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

### BACKGROUND

FIRST: On 12/20/2018, a claim was received from the claimant in which she indicated  
that in relation to the warning file A/211/2018, the cameras continue to  
located in the same place, without having been relocated.

Provide a photographic report made with a mobile phone camera in which the  
see a newspaper on 12/19/2018 and a gray stone block house in front with four  
windows. From a separation fence from the adjoining farms that can be seen in the photos  
to the house in which a device is placed there is a considerable distance, from  
so that it is not clearly appreciated that it is a video surveillance camera. All  
The images that it provides are of the same front and the same device.

SECOND: On 02/12/2019, a new letter was received from the claimant indicating that  
the cameras are still located in the same place, without having been relocated by their  
owners, A.A.A., and B.B.B., (hereinafter B.B.B. or the defendant) and that they continue  
capturing images of your property and of the people who move in said space.

Provides a photographic report in which a newspaper is viewed on 02/11/2019 and a house  
of gray stone blocks in front with four windows, perhaps more than forty feet into the  
first image in which it is verified next to the newspaper of 02/11/2019. The wall that is seen  
holds a device and is the same as the one contained in the claim In other  
photos is seen from an interior space with a white grill on the window, with the literal  
"From inside my girl's room" and in front you can see what could be the house of

blocks of gray stone, without it being clearly deduced in any of the photographs that

It is a video surveillance system.

Other writings of the same content were received from the claimant on 03/13/2019,

referred to the continuity of the situation as of 03/12/2019.

THIRD On 01/23/2019, the director of the AEPD agrees to admit the

claim and the claimant is notified.

FOURTH: From the resolution of the warning procedure A/211/2018 signed on

08/10/2018 highlights:

"In procedure A/00211/2018, instructed by the Spanish Agency for

Data Protection to B.B.B., (in view of the complaint filed by C.C.C. and under

of the following,"

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

2/14

Resolving:

COMPLY with the provisions of article 6 of the LOPD.

"1.- WARN Mrs. B.B.B. in accordance with the provisions of article 45.6 of the

Organic Law 15/1999, of 13/12, Protection of Personal Data, with

in relation to the complaint for violation of article 6 of the LOPD, classified as serious

in article 44.3.b) of the aforementioned Organic Law.

2.- REQUEST Mrs. B.B.B. in accordance with the provisions of section 6 of the

Article 45 of Law 15/1999 so that within a month from this act of

notification:

□

Specifically, the defendant is urged to either remove the cameras installed in the exterior of the farm, or reorient them, in such a way that images are not captured disproportionate amounts of the complainant's home.

REPORT to the Spanish Agency for Data Protection of compliance with

□

what is required, contributing in the event that you choose to remove the cameras, photographs of the place where they were installed before and after their removal, and to

In the event that you choose to redirect them, that you provide photographs with the images of the monitor in which it can be verified that images of the road are no longer captured

public or adjoining farms, as well as those documents in which

demonstrate compliance with what is required in the previous section.

You are informed that if you do not meet the aforementioned requirement, you could

incur in an offense typified in article 44 of the LOPD and punishable by

in accordance with the provisions of article 45 of the aforementioned Organic Law.”

#### PROVEN FACTS

FIRST: It is stated that on April 27, 2018 you have entered this Agency

letter from Ms. C.C.C., communicating possible violation of Organic Law 15/1999,

of December 13, motivated by video surveillance cameras whose owner is Mrs.

B.B.B., installed in \*\*\*ADDRESS.1.

Specifically, it denounces the installation of video cameras outside

the farm, being able to record images of the complainant's home.

Attached photographic report in which several cameras are observed

SECOND: It is established that the person responsible for the video surveillance cameras

located on the farm located at \*\*\*ADDRESS.1, is Doña B.B.B..

THIRD: It is established that on the farm to which the complaint refers there are

installed exterior cameras that are capturing images of areas

unrelated to the defendant, as they are located on the side façade with a focus on the complainant's home.

FOURTH: It is on record that the cameras installed on the façade of the property, due to its characteristics, its location outside the property and its orientation, can capture disproportionate images of areas outside the denounced, without authorization.

FIFTH: It is on record that on May 21, 2018 (and, secondly, on May 22, 2018), notification of the pre-procedure hearing agreement was attempted warning, to the address of the accused. Given the negative result of said The attempt was made, on June 11, 2018, to be sent to the Single Edictal Board of the aforementioned hearing agreement prior to the warning procedure for the denounced, for its publication in the Official State Gazette, a circumstance that

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

3/14

occurred on the XXX of 2018, granting the denounced term to carry out allegations to said agreement, ending the same without it being submit any writing.

SIXTH: Once the period granted for this purpose has elapsed, there is no record that the party denounced, no allegation has been presented.”

FIFTH: According to the consultation of the AEPD procedure management database, the agreement to start the procedure A/211/2018 of 05/17/2018, directed against B.B.B. was notified through BOE, having not picked up the notices at the Post Office.

On the other hand, with respect to the notification of the resolution of the procedure,

A/211/2018 addressed to B.B.B. something similar happened, it was returned as excess-not withdrawn- in the post office on 09/25/2018. The attempt to deliveries on 08/16 and 17/2018.

On 09/11/2018, the dictal notification appears in the BOE. Figure procedure A/211/2018, name or company name: L,P,R. and in NIF, \*

SIXTH: On 04/12/2019, the claimant indicates the Nif of the claimant and indicates that of the system

The name of the partner of the accused is the person in the contract "alarms".

SEVENTH: On 04/24/2019, the director of the AEPD agreed:

"Initiate disciplinary proceedings against B.B.B., for the alleged infringement of article 6.1 of the GDPR, punishable in accordance with the provisions of art. 83.5 of the aforementioned GDPR, and qualified very serious in article 72.1 a) of the LOPDGDD." opting as to sanction that could correspond to that of WARNING.

EIGHTH: On 5/10/2019, the defendant made allegations indicating:

The claimant's husband is her brother-in-law, her husband's brother, who maintain

1)  
"continuous false complaints that have been resolved in the Courts with sentences favorable to us."

2)  
The house was vandalized, so her husband hired a security service with SECURITAS DIRECT on 10/5/2016, "without any camera that captures images of the defendant's house, since the device that placed the company is volumetric photo, which is a class of photodetectors that is limited to "taking photos when you enter the farm. Indicates that if the limit is crossed, it does not occur

recording, but photographs are taken of when you enter your farm. Attach copy of contract of 5/10/2016 which includes the installation, maintenance and operation alarm center, with signs and an external perimeter detector with image. The external personal verification service of article 10.1.b) of the OM is included 316/2011 and does not include the key custody service 10.1.a of the aforementioned order). HE includes a "Securitas Direct alarm kit, connected to the network with a motion detector with color camera and flash" and another perimeter.

In the section on verifying alarm jump by SECURITAS, indicates that the central station will capture and record images of the devices installed in accordance with article 48 of the private security regulations.

"SECURITAS will keep the recordings obtained as a result of the alarm jumps generated by the installed system".

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

4/14

They provide photography of alarm system installation information.

"For the purposes of article 5.1 of Law 5/2014 of 4/04 on private security, the services that contracted are those included in letter f) and g)

f) The installation and maintenance of devices, equipment, devices and systems of connected to alarm receiving centers or control centers or video surveillance.

g) The operation of exchanges for the connection, reception, verification and, where appropriate, response and transmission of alarm signals, as well as monitoring of any signs of auxiliary devices for the safety of people, property

movable or immovable or compliance with imposed measures, and the communication to the Competent Security Forces and Bodies in these cases.”

3)

A copy of the installation and connection certificate signed by SECURITAS on 10/5/2016 indicating that the defendant's husband has contracted the provision of security services through an alarm center for the property located in (...) which coincides with the address of the CLAIMED.

The elements and devices installed correspond to security grade 2 established in Order INT/316/2011 of 1/02 on the operation of security systems alarm in the field of private security.” low to medium risk, dedicated to housing and small establishments, shops and industries in general, that intend to connect to an alarm center or, where appropriate, to a control center.”

It shows the installation of photodetectors, not including a video surveillance system.

NINTH: On 05/10/2019, a letter was received from the claimant stating that the violation persists.

Provide a copy of a photo that shows a wall other than the one in the initial photo, and a device that does not appear to be a video surveillance camera, indicating that it is "the alarm system support" and a visible metal fence as separation boundaries, indicating "photo where the security company initially installed said camera"

It provides the same photo as the one in the initial complaint, which does not look like a camera either of video surveillance on the defendant's facade, and a photo taken from the "room of his youngest daughter", and from another part of the façade with another device that can be seen from the door main of "my habitual residence"

TENTH: On 09/9/2019, a resolution proposal is issued with the literal:

"That by the Director of the Spanish Data Protection Agency it is

DECLARE, in accordance with the provisions of article 90.1 of the LPCAP, the non-

existence of responsibility on the part of B.B.B. of the violation of article 6.1 of the GDPR, typified in article 83.5 of the GDPR.”

In front of it, no allegations were received.

ELEVENTH: On 09/20/2019, a letter was received from the claimant that states:

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

5/14

You want to know the status of the claim.

to)

It generically requests that "if there is something in progress" it is sent to you.

b)

c)

Send photos in which it can be seen that there is a fence separating houses

with a green cloth, the house in which the device is located is in a higher area than

that of the defendant.

## PROVEN FACTS

1)

The claimant presupposes that her neighbor, with whom she borders her home on the land

adjoining has a video surveillance system arranged as it appears according to the photos it provides

some devices outside his home, stating that he is foreseeably

Focusing on parts of your home. In the images you provided you can see two frontals of the

defendant's house, and in one of them there is a device attached to the wall in a

front of the house. In the other photo a device on a beam. none of them can



verify that they are unequivocally video surveillance cameras.

According to the defendant, her husband and that of the claimant are brothers, and not

2)

They have a good neighborly relationship and have gone to court for "continuous" complaints.

3)

The house to which the complaint refers has contracted a security service

with SECURITAS DIRECT since 10/5/2016, "without there being any camera that captures

images of the defendant's house", since the device placed by the company is a photo

volumetric, a type of photodetectors that is limited to "taking photos when you enter inside

of the farm", with central alarm service, having posters. SECURITAS

custody of the recordings obtained as a result of the alarm jumps generated

for the installed system.

## FUNDAMENTALS 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 persons

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

these data (hereinafter GDPR); recognizes each supervisory authority, and as

established in art. 47 of Organic Law 3/2018, of 5/12, on Data Protection

Personal and guarantee of digital rights (hereinafter LOPDGDD), the Director of

The Spanish Data Protection Agency is competent to initiate and resolve

this procedure.

II

Regarding the situation of the claimant as an interested party

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

6/14

It must be taken into account that the procedure is initiated ex officio by agreement of the competent body, by complaint, and in accordance with article 62.5 of Law 39/2015, of 1/10 of the Common Administrative Procedure of Public Administrations: "The Submitting a complaint does not, by itself, confer the status of interested party in the procedure."

The claimant claims an alleged video surveillance installation that could Focus your property. This hypothesis is destroyed by the copy of the surveillance contract signed with the security company, certifying that it would not be security cameras video surveillance. Therefore, the mere complaint with assumptions that do not correspond to the facts revealed in the processing of the procedure have an impact on the condition of interested party, since not any and all presentation of a complaint must imply for the mere fact of its accreditation.

It is appropriate to reproduce the Judgment of the National Court room 1, of what contentious-administrative, appeal 786/2010 of 11/11/2011. So in its FOUNDATION OF SECOND LAW determines:

"To this end, it is necessary to bring up the STS of December 16, 2008 (Rec. 6339/2004 also issued regarding a resolution of the Director of the AEPD that agreed to file a procedure initiated by virtue of a complaint made by the appellants, and that it appreciated such lack of legal standing, by not justifying said actors that neither the opening of the disciplinary file nor the sanction of the denounced entity could produce a positive effect in the legal sphere of the same, or eliminate a charge or encumbrance in that sphere.

Judgment that, among others, contains the following considerations:

(...) in relation to the legitimacy in sanctioning matters and with respect to the complainants, this Chamber has been pointing out some criteria that make up doctrine jurisprudential and that allow to determine the concurrence of said procedural requirement. Thus, it is pointed out repeatedly, that it is about justifying the existence of a utility, position of advantage or real benefit, or more specifically, if the imposition of a sanction may produce a positive effect in the legal sphere of the complainant or may eliminate a charge or encumbrance, in that sphere (S. 5-23-2003, 11-28-2003, 11-30-2005, between others).

That for this reason the problem of legitimation has a casuistic nature, which is not allows an undifferentiated response for all cases, being necessary to examine in each of them the specific legitimate interest that justifies the legitimacy , incumbent on his allegation and proof to whoever claims it (SS. 11-21-2005, 11-30-2005), pointing out the judgment of November 3, 2005 that: (...) based on the fact that the answer to the problem of legitimation must be casuistic, so neither an affirmation nor a an undifferentiated denial for all cases, the Chamber understands that the existence of the legitimacy is linked to the legitimate interest of the party that arrogates it, being the key to determine whether or not that legitimate interest exists in the process of contesting a resolution (...) the data on whether the imposition of a sanction can produce an effect positive in the legal sphere of the complainant or can eliminate a charge or encumbrance in that sphere, and it will be like this, in each case, and depending on what is intended, how the

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

7/14

adequate response to such question, not being that the imposition of the sanction

constitutes by itself the satisfaction of an interest (...)

Thus, although there is no legitimacy to claim in the abstract the imposition of a sanction and, therefore, to initiate a disciplinary proceeding, it cannot be excluded that in certain matters the applicant may benefit from their rights or interests as a consequence of the opening of a disciplinary file (recognition of damages, right to compensation), which would grant legitimacy to request a certain inspection or sanctioning action (in this sense, Judgment of 14 December December 2005 - Rec. 101/2004).

However, the jurisprudence identifies in such judgments the scope of that legitimate interest of the complainant, considering as such (...) the recognition of damages or right to compensation and understanding that the allegation of that "the imposition of the sanction constitutes by itself the satisfaction of an interest" noting the judgment of November 26, 2002 that: "the complainant is not the owner of a subjective right to obtain a sanction against the accused, nor can it be recognized a legitimate interest in the success of your complaint, right and interest that are the presuppositions that configure the legitimacy, according to article 24.1 of the Constitution and Article 31 of Law 30/1992, without valid as holders of that interest the arguments referring to correcting the irregularities, or not to do so in the future produce, or to the moral satisfaction that the sanction would entail, or the investigation of the facts, for the complainant,..."

Along the same lines, and more forcefully, also the STS doctrine of 10/6/2009 (Rec. 4712/2005), also issued in a case very similar to the one now analyzed, also in terms of data protection, in which, after indicating that the The problem focuses on whether the complainants have active legitimacy to appeal via before the resolution of the Agency that puts an end to the disciplinary file initiated as a result of the complaint, the following is concluded:

“The answer must be unequivocally negative: whoever denounces facts that considered to constitute an infringement of data protection legislation lacks active legitimacy to challenge in court what the Agency resolves. Thus emerges from the judgments of this Chamber of November 6, 2007 and, more clearly still, of December 10, 2008. The reason is, in substance, that the complainant lacks the condition of interested party in the disciplinary procedure that can be initiated as a result of your complaint. Neither the Organic Law on Data Protection nor its implementing Regulations They recognize that condition. And as regards the general principles of law administrative sanction, although on some occasions this Chamber has said that the complainant can challenge the filing of the complaint by the Administration, it is not allowed that the complainant can challenge the final administrative resolution. The crucial argument in this matter is that the complainant, even when he considers himself a "victim" of the reported infringement, does not have a subjective right or a legitimate interest that the denounced is punished. Punitive power belongs solely to the Administration entrusted with the corresponding sanctioning power -in this case, the Spanish Data Protection Agency- and, therefore, only the Administration has an interest protected by the legal system in which the offender is penalized. Is It is true that things are not like that in criminal law proper, where there is even popular action; but this is because there are rules that expressly they establish exceptions to the public monopoly on the exercise of the ius puniendi; exceptions that do not appear in the penalizing administrative law and, therefore, now

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

specifically interested in the legislation on data protection. Furthermore: accept the active legitimization of the complainant would not only lead to sustaining that he has an interest that the legal system does not recognize or protect him, but would also lead to transform the contentious-administrative courts into a kind of organs of sanctions appeal. The latter would mean taking for granted that they can impose the administrative sanctions that the Administration did not impose, which would clash with the so-called "reviewer character" of the contentious-administrative jurisdiction. In other words, the contentious-administrative courts can and should control the legality of administrative acts in penalizing matters; but they cannot replace Administration in the exercise of the sanctioning powers that the law entrusts to that.

What has just been said must be clarified: the denouncer of a violation of data protection legislation lacks active legitimacy to challenge the Agency's resolution regarding the sanctioning result itself (imposition of a penalty, amount thereof, exculpation, etc.); but, if necessary, may have active legitimacy with respect to aspects of the resolution other than the specifically sanctioning provided, of course, you can show some genuine interest worthy of protection.

Given the necessary application of such doctrine of the High Court to the present case It turns out that in it, what the actor wants and requests, both in the plea of the lawsuit, as throughout the justification of it is the statement that the clinic denounced has violated article 6.1 of the LOPD, for having captured his images without their consent, arguing that when the Agency went to inspect such a clinic, five months after the events occurred, the reality was quite different, because in said time lapse they had created an appearance of having acted in accordance with the law. It turns out, therefore, that said complainant, according to the exposed doctrine, lacks

both of a subjective right and of a legitimate interest that the accused may be considered infringing of the LOPD, for which reason the exception of lack of active legitimation of Art. 69.b) of Law 29/1998 and, without the need for further considerations in accordance with the doctrine of the Supreme Court that has been exposed, the This appeal must be inadmissible."

The claimant will be informed when the resolution has been issued and that you can consult it on the web considering that article 6.1 of the GDPR, establishes the assumptions that allow the processing of personal data to be considered lawful. The provision of a detection system with a security company is covered for the legitimate interest on the part of the security company, and it is proportional since only Takes pictures in the event of a trespassing.

II

According to the data available, there has been evidence that in the house of the claimed there is a detection device that by movements, at a moment given would capture images that may contain personal data, that is, according to the definition of the GDPR, article 4.1: "any information about an identified natural person or identifiable ("the data subject"); An identifiable natural person shall be considered any person whose identity can be determined, directly or indirectly, in particular by means of a

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

9/14

identifier, such as a name, an identification number, data of location, an online identifier or one or more elements of identity physical, physiological, genetic, mental, economic, cultural or social of said person;

The purpose of the installation is to prevent trespassing on private property, for which which, only when the limit is crossed does it start working.

In accordance with Instruction 1/2006, of 8/11, of the Spanish Agency for Data Protection, on the processing of personal data for surveillance purposes through camera or video camera systems, article 1, indicates:

"1. This Instruction applies to the processing of personal data of images of identified or identifiable natural persons, for surveillance purposes through systems of cameras and camcorders.

The treatment object of this Instruction includes the recording, capture, transmission, conservation, and storage of images, including their reproduction or broadcast in real time, as well as the processing resulting from the personal data related to those.

A person will be considered identifiable when their identity can be determined through the treatments referred to in this Instruction, without this requiring disproportionate deadlines or activities.

The references contained in this Instruction to camcorders and cameras shall be understood also made to any analogous technical means and, in general, to any system that allow the treatments provided for in it."

As long as they meet the rest of the requirements, they could collect personal data.

staff, in addition to the classic closed-circuit television camera systems, the use of any fixed or mobile electronic system or element if it is capable of capturing data of images, for example portable cameras, webcams, or infrared cameras.

IV.

Law 5/2014, of 4/04 on Private Security indicates:

Article 5. Private security activities

"1. The following constitute private security activities:



f) The installation and maintenance of devices, equipment, devices and systems of connected to alarm receiving centers or control centers or video surveillance.

g) The operation of exchanges for the connection, reception, verification and, where appropriate, response and transmission of alarm signals, as well as monitoring of any signs of auxiliary devices for the safety of people, property movable or immovable or compliance with imposed measures, and the communication to the Competent Security Forces and Bodies in these cases.”

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

10/14

Article 32. Security guards and their specialty

"1. Security guards will perform the following functions:

f) Carry out, in relation to the operation of alarm receiving centers, the provision of personal verification services and response to alarm signals that Occur.

In addition, they will also be able to carry out the functions of reception, non-personal verification and transmission to the Security Forces and Corps that article 47.1 recognizes the security operators.”

Article 42. Video surveillance services

"1. Video surveillance services consist of the exercise of surveillance through systems of cameras or video cameras, fixed or mobile, capable of capturing and recording images and sounds, including any technical means or system that allows them treatments than these.

When the purpose of these services is to prevent infringements and avoid damage to the persons or goods object of protection or prevent unauthorized access, will be provided necessarily by security guards or, where appropriate, by rural guards.

The use of cameras or

video cameras whose main purpose is to check the status of facilities or goods, control of access to car parks and garages, or the activities that are developed from the control centers and other points, zones or areas of the highways of Toll. These functions may be performed by personnel other than private security.

2. Cameras or video cameras may not be used for private security purposes to take images and sounds of roads and public spaces or public access except in the assumptions and under the terms and conditions provided in its specific regulations, prior administrative authorization by the competent body in each case. Its use in the inside homes will require the owner's consent.

3. Video surveillance cameras that are part of security measures obligatory or reception, verification and, where appropriate, response and transmission systems of alarms, will not require administrative authorization for its installation, use or utilization.

4. The recordings made by video surveillance systems may not be used for a use other than its intended purpose. When they are related to criminal acts or acts that affect public safety, will be provided, on their own initiative or at your request, to the competent Security Forces and Bodies, respecting the conservation and custody criteria of the same for their valid contribution as evidence or proof in police or judicial investigations.

5. The monitoring, recording, processing and recording of images and sounds by of video surveillance systems will be subject to the provisions of the regulations on protection of personal data, and especially to the principles of

proportionality, suitability and minimal intervention.

6. In matters not provided for in this law and its implementing regulations, the

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

11/14

provided in the regulations on video surveillance by the Security Forces and Bodies

Security."

Article 46. Installation and maintenance services

"1. Installation and maintenance services of apparatus, equipment, devices and

security systems connected to central alarm receivers, control centers or

of video surveillance, will consist of the execution, by accredited technicians, of all those

installation and maintenance operations of said apparatus, equipment, devices or

systems, which are necessary for their proper functioning and good compliance

of its purpose, prior preparation, by accredited engineers, of the mandatory project of

installation, whose characteristics will be determined by regulation.

2. These systems must undergo preventive reviews with the periodicity and

manner determined by law."

Article 47. Alarm management services

"1. The alarm management services, in charge of security operators, will consist of

at reception, non-personal verification and, where appropriate, transmission of signals of

alarm, related to the security and protection of people and goods to the Forces and Corps

competent Security.

2. The alarm response services will be provided by security guards or, in

where appropriate, by rural guards, and may include the following services:

a) The deposit and custody of the keys of the buildings or objects where they are installed the security systems connected to the alarm center and, where appropriate, its transfer to the place from which the verified alarm signal or the opening to distance controlled from the alarm center.

b) The displacement of security guards or rural guards in order to proceed with personal verification of the received alarm.

c) Facilitate access to police or emergency services when circumstances require it, either through remote openings controlled from the alarm center or with the means and access devices available.

3. When the services refer to the analysis and monitoring of security events of information and communications, will be subject to the specifications that are determined by regulation. The alarm signals referring to these events must be brought to the attention of the competent body, when appropriate, by the user himself or by the company with which he has contracted the security.”

Order INT/316/2011, of 1/02, on the operation of alarm systems in the field of private security indicates:

Article 1. Material scope.

"1. Only authorized security companies may carry out security operations. installation and maintenance of security and alarm apparatus, devices or systems, when they intend to connect to an alarm center or to the so-called centers

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

12/14

of control or video surveillance that includes the first section of article 39 of the

Private Security Regulation.

2. In accordance with the provisions of article 46 of the Safety Regulations

Private, to connect appliances, devices or security systems to central alarms or control centers, it will be necessary for the installation to have been carried out by a security company registered in the corresponding Registry and conforms to the provisions of Articles 40, 42 and 43 of the aforementioned Regulation and the provisions of this Order.

Within the facilities that security companies can carry out there is the Alarm Receiving Center (art. 5.1.b) and 47 of Law 5/2014). The norm that specifically regulates these provisions (Order INT/316/2011, of 1/02, on operation of alarm systems in the field of private security) that the security company will proceed to verify the alarm that goes off in the place where the receiving center is installed before transmitting is to the Forces and Security forces. The form of verification can be any of those mentioned in the standard (sequential verification, verification by video, verification by audio or personal verification). As a complement -not a replacement- of said forms verification, the Order allows the alarm centers to call ("when deem convenient or necessary") to the telephone numbers (landline or mobile) provided by the owner of the installation in order to verify the veracity of the alarm received.

Article 8. Verification by video.

"1. To consider an alarm validly verified by this technical method, the video subsystem must be activated by means of an intrusion detector or a video sensor, it being necessary that the video coverage be equal to or greater than that of the associated detector or detectors.

2. The video verification process can only start when the signal of alarm has been visualized by the operator of the alarm center. Started the verification, the system must record a minimum of one image of the exact moment of the

alarm and two images after it, in a time window of five seconds,  
in such a way that they allow the identification of the cause that originated this.

3. The recording systems used for this type of verification will not allow  
obtain images of the monitored place, if an alarm has not previously occurred,  
unless you have the express authorization of the user or the standard requires a recording  
permanent."

In this case, it appears in the contract: "perimeter motion photodetector  
with color camera and flash and face-to-face verification service by a Securitas guard."

V

The service provided by security companies and its implications in terms of  
of data protection, in this case for the Installation and/or maintenance of the equipment and  
intrusion detection systems with use of equipment or access to images  
it's legit. These are security companies that in this case provide central service  
of alarms and image capture in photography mode, so that when the  
alarm jumps directly to the image that is viewed by the personnel of the  
security.

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

13/14

The GDPR defines "processor" or "in charge" as the natural person or  
legal entity, authority, service or other body that processes personal data on behalf of the  
responsible for the treatment. And "responsible for the treatment" or "responsible" is the  
natural or legal person, authority, agency or other body which, alone or jointly with others,  
determine the purposes and means of processing. In the present case, the personal data

obtained by the security company by signing the information contract provided by the user are not processed "on behalf of" the user, but said data personal data serve to establish a direct legal relationship between the company security and user. The security company uses the personal data for the establishment and fulfillment of the provision to which it is bound by the aforementioned service lease. Ultimately, the security company determines the purposes and means of processing said personal data for the provision of the obligated service.

In compliance with the provision to which the company is committed security through the service lease contract does not act "on behalf of" user, but rather provides the compromised security service, which constitutes the object own social security company." We are not, therefore, regarding said personal data, before a person in charge of the treatment. This means that the company security will have all the obligations of the person responsible for the treatment in relation to the personal data that it processes for the provision of the security service to the users of this Among them is that personal data is processed only for the specified, explicit, legitimate purposes for which they were collected (art. 5.1.b) GDPR), and not for purposes incompatible with them.

Contrary to what was denounced by the complainant, no images of permanent mode, because in the case of video detection when someone breaks into the installation, if there is a possibility that if it is accessed, images are taken that for a On the one hand, they serve to verify if the alarm jump is true, and on the other hand, they can identify or make identifiable the person who is trespassing on private property, with connection to State security forces and bodies. The basis of treatment is the defense of the private property as a faculty inherent to its owner, therefore legitimate interest. In this case, the person is not responsible for the system implanted.

denounced by the complainant. The contracted system is legitimate and the approach of the device is created to prevent intrusions into the property of the defendant, without its existence is proven to affect the rights of the claimant, for which reason your file comes.

Therefore, in accordance with applicable law

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARE, in accordance with the provisions of article 90.1 of the LPCAP, the non-existence of responsibility on the part of B.B.B. for the infringement of article 6.1 of the GDPR, in accordance with article 83.5 of the GDPR.

SECOND: NOTIFY this resolution to B.B.B.

THIRD: In accordance with the provisions of article 50 of the LOPDPGDD, the

This Resolution will be made public once the interested parties have been notified.

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

14/14

Against this resolution, which puts an end to the administrative process in accordance with art. 48.6 of the LOPDPGDD, and in accordance with the provisions of article 123 of the LPACAP, the Interested parties may optionally file an appeal for replacement 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 Court, with in accordance with the provisions of article 25 and section 5 of the fourth additional provision of Law 29/1998, of July 13, regulating the Contentious-Administrative Jurisdiction, within two months from the day following the notification of this act,



according to the provisions of article 46.1 of the aforementioned Law.

Finally, it is noted that in accordance with the provisions of art. 90.3 a) of the LPACAP, it may be provisionally suspend the firm resolution in administrative proceedings if the interested party expresses its intention to file a contentious-administrative appeal. If this is the one case, the interested party must formally communicate this fact by writing to the Spanish Data Protection Agency, presenting it through the Registry Email from the 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 October. You must also transfer to the Agency the documentation proving the effective filing of the contentious-administrative appeal. If the Agency did not have knowledge of the filing of the contentious-administrative appeal within a period of two months from the day following the notification of this resolution, would consider the injunction has ended.

Mar Spain Marti

Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](https://sedeagpd.gob.es)