 File No.: PS/00392/2020

- RESOLUTION OF PUNISHMENT PROCEDURE

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

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant), filed a claim on 06/22/2020 before the Spanish Agency for Data Protection. The grounds on which the claim is based are that "an illicit treatment of personal data has been carried out, consisting of the non-consensual capture of my personal image and voice data by recording video and its subsequent massive dissemination through social networks and the media".

He explains that he left (...) on ***DATE.1 “when I see a car marked by the police (...) from whose interior an agent signals me to approach the car”. identify several disclosures of the video on social networks, ***WEB.1 and ***DIARIO.1 in which it can be seen the video.

He points out that he found out because a few hours after it happened (10:30), they told him friends that the video was spreading massively on social networks, considering the claimant that the recruitment was made by the agent with “his mobile phone”.

In ***WEB.1, reference: “***REFERENCE.1” (…), profile “***PROFIL.1”, ***DATE.2, of duration, 34 seconds. Provide a copy of the CD in which the video that coincides with the the one that appears in ***WEB.1 and list of pages and media in which the video was broadcast.

It requests that a sanctioning procedure be initiated against those who are found to be violators.

SECOND: In view of the facts denounced in the claim and the documents provided by the claimant in accordance with the provisions of Title VII, Chapter I, Second section, of the Organic Law 3/2018, of 5/12 of Protection of Personal Data and guarantee of digital rights (hereinafter LOPDGDD), on 07/17/2020, the

claim to the CITY COUNCIL OF OVIEDO, (claimed) with the literal:

A response is received on 08/18/2020, stating that "on 8/10/2020 and after having

determined to the official of that Corps that could be the origin of the recordings

object of the complaint, he was informed that a copy of the complaint filed would be sent to him,

giving it until 8/13/20 to issue a report to that effect".

On 8/11/2020, the official appeared at the local police offices and was

submit the documentation.

It concludes that on 8/14/2020, said official stated that at the direction of his lawyer and

For the moment, it will not report on the claim transferred by the AEPD.

THIRD: On 10/22/2020, the claim is admitted for processing.

FOURTH: On 03/23/2021, the Director of the AEPD agreed:

“INITIATE PUNISHMENT PROCEDURE of a warning to the CITY COUNCIL OF

OVIEDO, for alleged violations of article 32 and article 5.1.f) of the Regulation

(EU) 2016/679 of the European Parliament and of the Council of 04/27/2016 on the protection

of natural persons with regard to the processing of personal data and the free

circulation of these data (hereinafter GDPR); in relation to article 5 of the Law

Organic 3/2018, of 5/12, on the Protection of Personal Data and guarantee of rights

(hereinafter LOPDGDD), as stated in article 83.4.a) and 83.5.a) of the

GDPR.”

FIFTH: On 04/13/2021, it presents allegations in which it states:

1-In the transfer of the claim it is not appreciated that the City Council appeared as

denounced for which proceedings were initiated to verify the identification of the alleged perpetrator of the recordings with your professional identification number. With this, it was understood that responded to the brief, and that it would serve as a basis to support the claimant's request in his duty to collaborate.

2- The claimant for the facts denounced requests how many investigative activities are consider accurate. They do not know if any investigative action has been carried out additional to the one sent by the City Council.

Considers that the rights and guarantees of any procedure have been violated recognized penalty in our legal system, since the Agency has not No investigation has been carried out to clarify the facts and the claimant has not requested to initiate proceedings against the defendant whom it does not indicate as alleged responsible. There is no minimum investigation of the facts before the start of the sanctioning procedure, which means that the burden of proof has fallen on the claimed, who is intended to be punished for some facts for which he is not responsible.

“It is clear from the facts contained in the claim that it was not the author or of the recordings or their dissemination. Nor does the defendant appear related to the media in which the images are disseminated, is not the owner of the media or page in which appear.

3- The facts related to the claimant's statement that the images were recorded from inside the police vehicle must take into account that the treatment of data is not municipal, these data are not included in any administrative file or hosted on their systems, so there has been no violation of security measures. claimant's safety.

4-There is no guilt in that the conduct that is reproached must be unlawful typified and guilty, consequence of action or omission attributable to the alleged offender, "for malice, recklessness, negligence or inexcusable ignorance”.

The City Council is being attributed the commission of some acts by the mere circumstance of

that the alleged perpetrator is a municipal worker who eludes the basic principle of

sanctioning regime and also the Data Protection regulations themselves, as they are contrary to

the definition of data controller contained in article 4 of the Regulation, since

the images are not captured or disclosed by the claimed party.

The assumption of responsibility for the acts committed by a public official in a

act of service cannot be considered direct, but subsidiary. In case of

existence of an offense is not automatic either, but rather requires an analysis of the situation.

It would be necessary that the sanctionable act occurred in the performance of its own functions

of the police misusing their public function with a lack of due observance

and diligence in the control of the employee's performance by the administration,

all the concurrent circumstances of the denounced facts must be assessed. Is

assessment of the concurrent circumstances has been obviated in the procedure.

5- The means by which the recordings were made does not come from the municipal system,

because they lack corporate mobile devices through which they can do

recordings.

The alleged recording and dissemination of a verbal warning made by an agent to a

citizen that is what the complaint consists of in this case, exceeds the functions

typical of any municipal employee, especially a police officer, since they do not

There are instructions issued by superiors or by any municipal official that

order the capture and dissemination of images of people detained or warned as

test medium.

There is no link between the functions of the police and the recording and dissemination of the images since there was no need to make such recordings for incorporation into a diligence or administrative file, nor do the agents have corporate means to be able to catch them.

6-The video continues to be exposed, although the AEPD has a "priority channel" to communicate the dissemination of sensitive content and request its withdrawal, with a series of mechanisms tending to its withdrawal, and if appropriate, a sanction against the people who have disseminated this material.

7-They have technical and organizational security measures in accordance with the annex two of the National Security Scheme, and develops a training plan for employees that includes online training material and reinforcement with training courses specialized in Data Protection.

8-Given that it is not considered responsible for the treatment or the dissemination of the images or of its recording, "I have not been able to incur in the imputed infractions". Request the file process.

SIXTH: On 04/14/2021, it was decided to carry out tests, incorporating the claim and the documentation obtained from the transfer as well as the allegations to the initial agreement.

In addition, the respondent is requested to report:

a) If the Agents have written instructions or any other means, on the use of the personal data of citizens, specifically with the use of devices such as

personal mobiles, when they are on public roads providing service, how have they been provided that information?

A response is received on 05/06/2021, indicating having received the request for evidence and state that these are “allegations”.

It shows that in the allegations to the initial agreement of 04/14/2021 they requested that investigate the facts, considering it as a request for evidence and it has not been done, and that Those allegations went unanswered. The actions of inspection of the AEPD that is said in the test agreement: they are considered reproduced "the documents obtained and generated by the Inspection Services before the City Council”, and they do not know if that Service carried out inquiries, not being able to allege or request evidence related to them, since it is unknown if such an inspection was made or what inquiries figure.

Regarding what was requested, it states that the employees of the City Council have information that can be seen on a website of the municipality, on the use of devices "code telematic”, within the transparency section. The link offered, when clicked, takes you to the page of the claimed but not directly to the information, giving an error, ignoring at the organization and security measures in terms of data protection that information and Through what means is it given to employees, to local police officers in particular.

In addition, he points out, the police group to which the alleged author of the recordings belongs sent instructions on the use of the images in email on 11/22/2017. I know I attach a copy of the email sent as an email with instructions on the use of images. The instructions refer to a "guide to the use of mobile camcorders by the Security Forces and Bodies”, which was also posted on the order board of the center along with a report from the City Council Advocacy on the use of private video cameras of police officers as a means of defending complaints.

It accompanies the emails, and it is appreciated that originally part of a union

police that bears the literal "look at the attached document", entitled "guide for the use of video cameras mobile by the security forces and bodies". In turn, from the Local Police Headquarters, sent to various addresses and people, and on 11/22/2017, it was sent to various groups of police recipients.

a) If there is any reference typified in the applicable regulations in compliance with the provision of the service, which can be adjusted to the case in which an agent that captures presumably with his private cell phone to a person from inside the police vehicle, which then also appears on ***WEB.1, for no reason, what kind of infraction could it be? It states that the file is in the initiation phase and that at the current date it is not possible identify the infringement without violating the rights of the alleged author of the recording, sanctioning procedure established in Organic Law 4/2010 of 20/05, of the disciplinary regime of the National Police Corps.

b) If that entity, about the alleged author of the capture of the images that are later disseminated, has initiated disciplinary actions or of any other type, either ex officio or by request of the affected

He stated that: "The ENS Security Committee of the City Council of Oviedo in a meeting of 16 of April 2021 has reached an agreement and sent a communication to the Chief of the Local Police, urging the performance of pertinent actions of at least the opening of a file information to the alleged perpetrator of the events while the Agency carries out the investigations about them that are relevant to establish authorship."

In the proposal that it provides, it is indicated that the transfer of the claim was received on 08/06/2020

of the Spanish Agency for Data Protection and is proposed to the local police officer who identifies himself,

for the possibility of having made an illicit treatment of data through the mobile phone

and its subsequent dissemination, involuntary capture of personal image and voice data through

video recording by mobile phone and its subsequent broadcast.

It states that: “On May 3, 2021, the Chief of the Local Police proposed

initiation of disciplinary proceedings against the allegedly implicated agent”. Although it indicates that

a copy is provided, the document that it indicates has 22 pages, it is cut on page 9, being able to

not having attached the document correctly.

He states that there is no record of the authorship of the broadcast of the recording since until

the date the City Council lacks information on who spread the video on the networks

requiring the Agency to carry out timely investigations.

It also requests that the term for carrying out the test be extended up to the limits

maximum, so that the Agency can make pertinent inquiries about the facts.

Request that the Agency investigate the facts by providing sufficient evidence of the authorship to the

less than the dissemination of the videos, sending the result of said videos to the City Council

investigations so that they can be presented as evidence in the procedure

sanctioning party and, where appropriate, in the file of the alleged offender, exonerating the City Council

responsibility for recording and broadcasting the video.

SEVENTH: On 11/3/2021, a resolution proposal is issued with the literal:

“That the Director of the Spanish Data Protection Agency direct a

warning to CITY COUNCIL OF OVIEDO, with NIF P3304400I, for infractions of the

GDPR of articles:

- 32 of the RGPD, in accordance with article 83.4.a) of the RGPD,

- 5.1.f) of the RGPD in accordance with article 83.5.a) of the RGPD”

Faced with the proposal, allegations are received on 11/19/2021, in which it states:

– “Inconsistency of the Resolution proposal with the claim presented by the

affected that gives rise to the initiation of the file, contravening article 88 of the LPACAP. In

the resolution proposal only deals with capturing the image, without assessing the

dissemination that is also part of the object of the claim with the publication on networks

social networks, internet or media of the image of the claimant."

-"Dissemination treatment is not taken into account nor have actions been taken to

stop the publication of images in the media. Thus, from July 17, 2020,

date of registration of the claim, as of November 15, 2021, the video of the

claimant is still published."

- "Breach of the principles of the sanctioning procedure in the sanction proposal

to City Hall. Taking into account that the damage to the interested party is not produced so much by the recording

but by the dissemination of images, it is necessary to reiterate that, among the principles of

sanctioning power included in Law 40/2015, of October 1, on the legal regime of the

public sector, the principle of necessity is found in its article 29 in which paragraph 3

points out: "In the normative determination of the sanctioning regime, as well as in the imposition

of sanctions by the Public Administrations, the due suitability and

necessity of the sanction to be imposed and its adequacy to the seriousness of the constitutive act of the

infringement".

-Reiterates that:

 "It is not considered responsible for the treatment of recordings that are not

made in the performance of their duties. The City Council is not responsible for the

purposes - unrelated to the needs of performing the job -, nor of the means of recruitment -

the device is owned by the employee- nor of those of dissemination identified by the claimant.”

 “The making of the video is not a consequence of an action or omission of the

City Hall of Oviedo. The City Council does not authorize members of the local police to

make recordings for purposes other than traffic control or public safety, or

It is a performance framed in their professional functions. The derivation of the

responsibility to the City Council for some facts that it has not committed bankruptcy the principles

of the sanctioning procedure since, according to the jurisprudence, “[…] otherwise,

would collapse the foundation of the punitive system, according to which each one responds of his

own acts, without it being possible, in order to more effectively protect public interests,

establish any liability punishable jointly and severally for acts of others”.

 Absence of responsibility, either by intent or by fault or lack of diligence in the

compliance with obligations in terms of Data Protection.

-They consider regarding the manifestation that they have acted with delay in taking

specific measures in the initiation of the disciplinary procedure against the alleged

responsible for the video, which has not been the case, since in the transfer phase of the claim

communicated to the Agency the identity of the person who had allegedly carried out the

recordings and it is the only one that has powers and competences for the investigation

in terms of data protection, the City Council lacking any means of proof

against the agent beyond the viewing of the image and the claim, proceeding to the

collaboration with the Agency.

When the City Council was aware that the AEPD was not going to carry out any investigation

additional "initiated the procedures for the opening of the sanctioning procedure, indicating that

in it "a statement has been taken from the alleged perpetrator."

They provide a copy of a letter dated 04/30/2021, communicated to staff of the "proposed initiation of disciplinary proceedings" in which the beginning of the actions of the AEPD received on 08/06/2020 and "having seen the report issued by the Head of the Unit of Technical office of 08/15/2020" narrating the facts of the transfer of the claim to the police and his posture.

-To justify that you have technical and organizational measures in data processing provide an ANNEX 1 on the training given in security and data protection from May 2018, noting that more than 500 employees have attended the face-to-face actions. To this must be added the activities carried out especially for the local police, with face-to-face training for a total of 30 troops, with specialized courses on cybersecurity, social networks or minors. In addition, online training was given open to any employee, including local police. The ANNEX does not indicate how many members make up the local police, offering the number of employees who have carried out the training actions throughout the editions of the various actions in each year. Other different box specifies the training actions of the local police, appearing in 2018, eight people, in 2019, one, in 2020 six and in 2021, one.

PROVEN FACTS

FIRST: The claimant claims for the fact of "the involuntary collection of my data personal image and voice by video recording" and "its subsequent massive dissemination to through social networks and media". He explains that it came out (...) on ***DATE.1 and Signals were made from a Local Police car for me to come closer" to the car. I know can see the video, indicates the claimant in ***DIARIO.1, or "on social networks such as ***WEB.2, ***WEB.3, ***WEB.4, ***WEB.1", as indicated. In ***WEB.1, it can be seen that the video is made from inside the vehicle of the Local Police, it also makes it

manifest in the claim by the claimant, specifically from the passenger seat. is captured to the person (…) from the front, the claimant. As you move to the left side of the vehicle, the shot that always focuses on him moves, and warned, he stops. the agent of police driver of the vehicle, who is also recorded from the side speaking through the window, (...) and the claimant (...) of his own accord turns towards his house. When retires is also followed in his departure by the camera. You can hear perfectly conversation and the claimant is fully identified.

THIRD: In the transfer of the claim, the respondent stated that he had been able to identify the official who could be the source of the recording to whom he delivers the request, and that he declined to make any statement on the case.

FOURTH: The defendant, in the request for evidence initiated on 04/14/2021, stated, dated 05/06/2021, that “The ENS Security Committee of the Oviedo City Council in a meeting of 16 of April 2021”, “has reached an agreement and sent a communication to the Chief of the Local Police, urging the performance of pertinent actions of at least the opening of a file informative to the presumed author of the facts.”

In execution of the measure, “On May 3, 2021, the Chief of the Local Police proposed initiation of disciplinary proceedings against the allegedly implicated agent.”

FIFTH: Requested in tests, if the claimed, as responsible for the treatment of the data carried out by its Agents, it has given these instructions on the use of the data citizens, specifically with the use of devices such as mobiles personal, when they are on public roads providing service, their response was that

sent on 11/22/2017 a document entitled "guide for the use of mobile video cameras by Forces and Security Bodies", of which its content is ignored or responsible for editing and contents. The guide came from a Police Union targeting emails from employees and Police of the City Council, who forwarded it to other mailing lists by Police groups/scales. Its content, elaboration and in any case, its origin is unknown. comes from the person in charge charged in this procedure, being a document also prior to the entry of the RGPD, applicable as of 05/25/2018.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each control authority, and as established in arts. 47 and 48.1 of the LOPDGDD, the Director of the Agency Spanish Data Protection is competent to resolve this procedure.

II

Regarding the allegations of the respondent regarding the need to carry out actions of investigation, indicate that if they were mandatory, they should have been carried out before the initial agreement, not at the pretrial phase.

"Prior to the initiation of the procedure, preliminary actions may be carried out ways in order to determine on a preliminary basis whether there are circumstances that justify quen such initiation (article 55 of the LPACAP). In particular, these actions will be aimed at determine, as precisely as possible, the facts likely to motivate the initiation of the procedure, the identification of the person or persons who could be responsible bles and the relevant circumstances that concur in each other."

The previous actions will be carried out by the bodies that have been assigned functions of investigation, inquiry and inspection in the matter and, failing these, by the person or administrative body that is determined by the competent body for the initiation or resolution tion of the procedure.

Preliminary actions do not constitute a proper phase of the administrative procedure.

nistrative sanction since, as we have pointed out, their purpose is to determine with

preliminary character if the circumstances that justify the initiation of the procedure concur.

I lie.

The LOPDGDD on previous investigation actions indicates in article 67:

"1. Before the adoption of the agreement to initiate the procedure, and once admitted for processing

the claim, if any, the Spanish Data Protection Agency may carry out

preliminary investigative actions in order to achieve a better determination of the facts and

the circumstances that justify the processing of the procedure”

Once in the instruction phase of the sanctioning procedure, the following are applicable:

general principles of criminal law with nuances. During the training phase they have

place the actions to verify the facts and allegations and ends the investigation

with the resolution proposal that will establish “in a reasoned manner the facts that are considered

proven” and its exact legal qualification, the infraction that, in its case, will be determined.

those constitute, the person or persons responsible and the proposed sanction, the

evaluation of the tests carried out, especially those that constitute the foundations

basics of the decision” (art 89.3 LPACAP).

The facts that motivate the initiation and imputation of responsibility to the defendant appear

clear in the initial agreement. These facts were known by the defendant through the

claim transfer. At no time did they mention the authorship of the exposed video

but the very making of the video, as it derives from what is seen on ***WEB.1 and what is captured

from inside the vehicle the images of the claimant.

In the testing period of this procedure, it is not appropriate as requested by the

demanded that the authorship of the exhibition of the video be investigated, to which the

fundamentals of the initiation agreement, but only to authenticate that the images were obtained

from within.

III

Within the definitions, the GDPR points out:

Article 4:

1) “personal data”: all information about an identified or identified natural person.

ble ("the interested party"); An identifiable natural person shall be deemed to be any person whose identity

identity can be determined, directly or indirectly, in particular by means of an identifier,

such as a name, an identification number, location data, an identity

online maker or one or more elements of the physical, physiological, genetic identity,

ca, psychic, economic, cultural or social 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;

7) “controller” or “controller”: the natural or legal person, authority

public, service or other body that, alone or jointly with others, determines the ends and means

of the treatment; if the law of the Union or of the Member States determines the purposes and

means of treatment, the person responsible for treatment or the specific criteria for its

appointment may be established by the Law of the Union or of the Member States;

9) "addressee": the natural or legal person, public authority, service or other body to which
that personal data is communicated, whether or not it is a third party. However, it is not
The public authorities that may receive personal data in the
framework of a specific investigation in accordance with the law of the Union or of the
Member states; the processing of such data by said public authorities will be
in accordance with the rules on data protection applicable to the purposes of the treatment-
I lie;

10) "third party": natural or legal person, public authority, service or body other than the
The interested party, the person in charge of the treatment, the person in charge of the treatment and the persons
entities authorized to process personal data under the direct authority of the controller or
of the manager;"

The distinction between data controller and employee of the latter is derived from the GDPR, which
has the effect of being authorized to process personal data under its authority and in its
Name. Data processing is not carried out solely by the controller or the person in charge.
of treatment, but rather the number of users who process personal data in any
Any public administration is equivalent to the number of public employees of the same.
With this, it is meant that both the decision-making positions of responsibility and the employers
employees acting on behalf of the data controller, when carrying out data processing
of personal data in the performance of their duties, within their structure.
ra, they are in the circle of power of direction and action of said person in charge of the treat-
also in what affects the implementation of its data protection policy
(data governance).

The RGPD or the LOPDGDD at no time determine that the responsibility in the

treatment may be required of the employee or position, if it refers to the responsibilities

disciplinary measures in article 77 of the LOPDGDD that referring to the processing of personal data

personal character by public entities, specifies:

"two. 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

competent data protection authority will issue a resolution sanctioning the

themselves with warning. The resolution will also establish the appropriate measures

adopt to stop the behavior or correct the effects of the infraction that had occurred.

task.

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.

3. Without prejudice to what is established in the previous section, the data protection authority

It will also propose the initiation of disciplinary actions when there are indications

enough for it. In this case, the procedure and the sanctions to be applied will be the

established in the legislation on the disciplinary or sanctioning regime resulting from

app.

Likewise, when the infractions are attributable to authorities and managers, and it is proven

the existence of technical reports or recommendations for treatment that would not have

been duly attended to, the resolution in which the sanction is imposed will include a

reprimand with the name of the responsible position and the publication will be ordered in the

Official Gazette of the State or regional government that corresponds”

Responsibility is demandable to the person in charge of the treatment, regardless of the fact that

have the personal data by itself, decision of its Director or titular position, as if the decision

sion is taken by an employee, especially if it occurs as in this case, in the development of the

assigned professional duties.

IV

Article 5 of the RGPD refers to the principles related to the processing of personal data, and

in its number 2: "The data controller will be responsible for compliance with the

provided for in section 1 and capable of demonstrating it (“proactive responsibility”)”, known

as "compliance" that could be equivalent to, not only compliance, regulatory in this case,

but also in prevention and responsibility of the members that make up their

organizations and the total commitment of their leaders, a mechanism to ensure

good governance and regulatory compliance regarding data protection.

The origin of this action measure arises from requiring companies to implement these

those of compliance to avoid the so-called "self-endangerment" that may suppose that

executives or persons with express powers of attorney to perform functions, may find

provide facilities to carry out behaviors of falsehood in commercial documents and scams

in medial competition, incorporating the Penal Code in its article 31 bis. as modality

of prevention, deploying effective a priori controls and being able to assume its im-

effective enforcement of regulatory infractions. From there arises the figure of the "compliance officer"

that is inserted in a supervision and control body that ensures compliance with the plan of

prevention; commissioning said person, these tasks with autonomy and independence.

Within this system, the establishment of a disciplinary system that sanctions

non-compliance with the measures established by the model", as a form of

to persuade employees to comply with the code of ethics and crime prevention, and

as an expression of a true zero tolerance policy towards the commission of infractions

of criminal relevance, foreseeing measures against people who seriously fail to comply with

crime prevention system

With Directive 95/46/CE of the Parliament and of the Council, of 10/24/1995, regarding the

Protection of Natural Persons with regard to the processing of personal data and

the free circulation of these data-and the consequent Organic Law 15/1999, of 12/13

protection of personal data, the data protection model was based on

a “static” scheme of the security measures to be implemented, depending on the type of

the data processed, the aim was to avoid the infringement of the rights of the interested parties as

primary obligation.

With the RGPD, anticipation of the infringement or injury of rights is sought, compliance

in advance to avoid injury or infringement of the right or freedom of the interested party. Yes

well, the RGPD/LOPDGDD binomial does not specifically list what those measures are

to implement, does not focus on information belonging to the organization

(public or private), but is especially linked to the protection of the data of the

natural persons, demanding a proactive responsibility, and not a reactive responsibility,

as in the previous model. This proactive approach to “implementation

permanent” of the security measures, implies that they are no longer static (as

in the previous model), but dynamic, corresponding to the data controller

determine at all times which of those security measures are necessary to

guarantee the confidentiality, integrity and availability of personal data, being

The first step is to carry out a 'risk analysis'.

Once such threats have been evaluated, the person in charge will be able to determine what are the measures most appropriate to mitigate or eliminate the risks for the treatment of data that may arise and affect the rights and freedoms of natural persons.

Consequently, proactive responsibility is required, rather than reactive (risk-based approach), having to act preventively, having the due diligence to avoid unwanted processing or breaches in the protection of the interests of citizens in the field of privacy.

It is the person in charge or in charge of treatment who must accredit said diligence with a solid and effective internal control system. Therefore, mere demonstration will not suffice. formal compliance, but this principle requires a previous, conscious, diligent attitude and proactive by organizations against all data processing personal they carry out.

Whether these measures are mandatory, or how they are applied, will depend on factors that must be taken into account in each case, such as the type of treatment and the risk that said treatment implies for the rights and freedoms of the interested parties. Consequently, due diligence, must be adapted to the level of risks in the protection of data and the organization characteristics.

The concept of due diligence can be defined as “the measure of prudence, activity or assiduity that can reasonably be expected, and with which it normally acts, a organization prudently and reasonably in certain circumstances; it is not measured by an absolute norm, but depending on the relative facts of the case in question”. By Therefore, due diligence is a process in continuous observation and prevention of the effects negative aspects of the activities of the entities on data protection.

Due diligence in data protection:

-It must cover the possible negative consequences on data protection that the

company could cause or contribute to cause through its own activities or

omissions, which are directly related to its operations, products or services

borrowed.

-Will vary in complexity depending on the size of the organization, the risk of serious

negative consequences on data protection and the nature and context of their

operations.

- It should be a continuous process, since the risks can change over time, depending on the

function of the evolution of the operations and the operational context of the organizations.

Accordingly, due diligence is made up of four elements: identify, prevent,

mitigating and accountability, i.e.:

1. An assessment of the actual and potential impact of the activities on the data

(Risks evaluation).

2. The integration of the conclusions, and the action in this regard (controls).

3. Follow-up and monitoring (performance evaluation).

4. Communicating how you deal with negative consequences

(accountability).

Due diligence provides a defense against liability, allows

reduction of sanctions or provides a defense remedy when the company can prove

that it had implemented “adequate procedures” to prevent an impact.”

In order to prove due diligence, the entity must demonstrate that it has given all the

reasonable steps and taken the necessary actions to avoid generating a

negative impact. This will be interpreted depending on the specific circumstances of each case.

The Regulation intends to anticipate the moment in which the person in charge or in charge of the treatment acts with due diligence, through this principle of proactive responsibility, managing the risks through a solid internal control system, which allows to certify this diligent action in advance, which initially, may present some uncertainty in its application, due to the passage of a closed system, based on a specific enumeration of the security measures to be implemented depending on the type of processed data, to an open system, whose objective is the application of technical measures and "appropriate" organizational structures to guarantee and be able to demonstrate that the treatment is adequate according to the scope, context and purposes of the treatment.

For the fulfillment of the principle of "Proactive Responsibility" the person in charge and in charge of treatment must previously carry out an analysis and study of compliance in terms of risk-based data protection. In other words, they must analyze what measures of data protection are necessary to implement to ensure compliance with the Regulation, depending on the nature, scope, context and purposes of the treatment of data that they carry out, as well as the risks (probability and consequence) of interference in the rights and freedoms of the interested parties.

In this way, the more probable and greater the consequences of the risk of the treatment, more or more far-reaching measures must be necessary to implement to counteract them (it should be clarified that these are not only security measures technique).

The risk-based approach is configured as a key factor in the process of
adequacy or compliance with data protection regulations, since all responsible
or person in charge must previously analyze the level of risk in which the
treatments. As a consequence, the RGPD establishes the obligation of those responsible and
responsible for implementing an internal system of compliance with regard to the protection of
data. System that will be integrated by different internal privacy policies or processes
which must be periodically updated and audited in such a way as to demonstrate
compliance with the Regulation.

Law 40/2015, of 1/10 of the Law on the Legal Regime of the Public Sector, states in its article
the 28.4:

“The regulatory laws of the different sanctioning regimes may classify as
infraction breach of the obligation to prevent the commission of infractions
administrative by those who are subject to a relationship of dependency or bond.
Likewise, they may provide for the cases in which certain persons will be responsible for the payment
of the pecuniary sanctions imposed on those who depend on them or are linked to them.”

v

For the recording of the personal data of the claimant embodied in the images of the
video that has been previously identified, the Oviedo City Council is charged with the infraction
of article 32 of the RGPD, which indicates:

"1. Taking into account the state of the art, the application costs, and the nature, the
scope, context and purposes of the treatment, as well as risks of probability and severity
variables for the rights and freedoms of natural persons, the person in charge and the
in charge of the treatment will apply appropriate technical and organizational measures to
guarantee a level of security appropriate to the risk, which, where appropriate, includes, among others:

a) pseudonymization and encryption of personal data;

b) the ability to ensure confidentiality, integrity, availability and resilience

permanent treatment systems and services;

c) the ability to restore the availability and access to personal data in a

fast in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment of the effectiveness of the

technical and organizational measures to guarantee the security of the treatment.

2. When evaluating the adequacy of the level of security, particular consideration will be given to the

risks presented by the processing of data, in particular as a consequence of the

accidental or unlawful destruction, loss or alteration of transmitted personal data,

stored or otherwise processed, or unauthorized communication or access to such

data.

4. The person in charge and the person in charge of the treatment will take measures to guarantee that

any person acting under the authority of the person in charge or the person in charge and

access to personal data can only process said data following instructions from the

responsible, unless it is obliged to do so by virtue of Union Law or the

Member states."

In relation to adopting the corresponding security measures, the RGPD seeks to take advantage of

the advantages offered by risk management, but introduces a new vision, where the focus

of attention is not focused on the threats that hang over the company, focusing its

attention to threats to the rights and freedoms of the interested parties. The evaluation

of the risks must be the result of a reflection on the implications that the

processing of personal data have on the interested parties. Is about
establish to what extent a treatment activity, due to its characteristics, the type of
data to which it refers or the type of operations can cause damage to the interested parties.
This approach involves estimating the damage and the type of damage that can occur on the
interested parties, for example, material damage arising from the violation of their rights and
freedoms, or your privacy. Therefore, and before the adoption of the aforementioned measures,
must proceed to assess the risk inherent in the treatments.
Recital 74 of the RGPD says that it indicates: "The responsibility must be established
of the data controller for any processing of personal data carried out by him
yourself or on your own. In particular, the person responsible must be obliged to apply measures
timely and effective and must be able to demonstrate the conformity of the activities of
treatment with this Regulation, including the effectiveness of the measures. These measures
must take into account the nature, scope, context and purposes of the treatment as well
as the risk to the rights and freedoms of natural persons." (The underlining is from the
AEPD).
Any of these employees may perform data processing that is not in accordance with
me with the personal data protection regulations, either through the means provided
nates or others, so privacy training should be integral to the
virtually all members of the organization.
The person in charge must establish information and training of its employees in the matters,
guidelines and dissemination of information on data processing, so as to achieve
a uniform application in its field.
Even so, employees and management positions must consider before proceeding to a
data processing, especially if it is different from the usual, or novel, by interpretation
or due to a specific situation, carry out a consultation with the data controller beforehand. East
must issue rules to its employees and management centers to coordinate basic aspects

of data processing.

Apart from the knowledge that must be provided and presupposed to the policemen about the

capturing images on public roads by the Security Forces and Bodies, which is governed

by its specific legislation, constituted by Organic Law 4/1997, of August 4, by the

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

public places, logically the consequences of the

use of personal mobile devices. On these, except for the use that can be made of the

called institutional for the exercise of functions in the cases in which

may be accurate, it must be indicated that their use, such as cameras or personal mobile phones of the

agents for capturing images in the development of professional work, does not guarantee the

data security, while the private uses that each agent can perform with

their own devices are not compatible with the security measures that for the

exercise of police functions must be adopted by those responsible for treatment,

having to accommodate and anticipate specific responsibilities and sanctions in its case. In this

case, it is proven that there are no such measures that have involved an unlawful interference

in the data protection right of the claimant.

In this case, it is not proven that the defendant had measures in place on the use

of personal devices in relation to the performance of their tasks, where they warned of their

regime of use and sanction, or the non-necessity or proportionality of recording images

such as the one that has been the subject of this claim. The due diligence regime

of the principles of data processing is related to the adoption of these protocols,

considering that the rights of citizens can be affected. The infringement of

this article.

Otherwise, the initiation of the disciplinary process, which is only one part of the policy of

regulatory compliance in the organization, is revealed late, and reactive, since it has been with

occasion of the practice of tests, when it is proven that there is no specificity relative to

security measures in the development of the tasks entrusted according to the

risks and devices.

SAW

The author of the video that is viewed on ***WEB.1 provides services for the defendant, and is charged

to the CITY COUNCIL OF OVIEDO the infringement of article 5.1.f) of the RGPD:

“Personal data will be:

“processed in such a way as to ensure adequate security of personal data,

including protection against unauthorized or unlawful processing and against loss,

accidental destruction or damage, through the application of technical or organizational measures

appropriate (“integrity and confidentiality”).”

The LOPDGDD states in its article 5:

"1. Those responsible and in charge of data processing as well as all persons

that intervene in any phase of this will be subject to the duty of confidentiality to which

refers to article 5.1.f) of Regulation (EU) 2016/679”

We are not talking here about the author of the broadcast of the video that appears on ***WEB.1, but about something

previous

without whose registration it would not have been possible and of data that have escaped the control of their

authors. This procedure is about the treatment derived from the collection of images

taken, without a doubt, from inside the vehicle, which coincides with the exposed video,

as can be seen from the same vision of the video. Deliberate and clear capture that collects

personal data of the claimant, he can be identified and located on public roads. Is

image only has one origin, which is that of the agents who at that moment speak with the claimant. It is appreciated that the total image of the agent sitting in the seat is collected driver of the stationary vehicle and this is the one who speaks to the claimant. The image had to be captured by his companion, given the angle of the images he collects. The collection of image is what then makes it possible for it to circulate on ***WEB.1 and on other social networks.

SAW

Article 83.4 a) of the RGPD indicates: “Infringements of the following provisions are sanctioned, in accordance with paragraph 2, with administrative fines of EUR 10,000,000 maximum or, in the case of a company, an amount equivalent to 2% as maximum of the total global annual turnover of the previous financial year, choosing for the largest amount:

“The obligations of the person in charge and the person in charge under articles 8, 11, 25 to 39, 42 and 43;”

For prescription purposes, the infringement of article 32 is contained in article 73 f) of the LO-PDGDD, which determines:

“Based on the provisions of article 83.4 of Regulation (EU) 2016/679, they are considered serious and will prescribe after two years the infractions that suppose a violation substance of the articles mentioned therein and, in particular, the following:

The lack of adoption of those technical and organizational measures that are appropriate to guarantee a level of security appropriate to the risk of the treatment, in the terms required by article 32.1 of Regulation (EU) 2016/679.”

While article 83.5 a) of the RGPD indicates:

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

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

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

annual global of the previous financial year, opting for the highest amount:

“the basic principles for the treatment, including the conditions for the consent to

tenor of articles 5, 6, 7 and 9;”

For prescription purposes, the infringement of article 5.1.f) is contained in article 72. 1.a) of

the LOPDGDD, which determines:

“Based on the provisions of article 83.5 of Regulation (EU) 2016/679, they are considered

very serious and will prescribe after three years the infractions that suppose a violation

substance of the articles mentioned therein and, in particular, the following:

The processing of personal data violating the principles and guarantees established in the

Article 5 of Regulation (EU) 2016/679.

Article 58.2 of the RGPD provides: "Each control authority will have all the

following corrective powers indicated below:

b) send a warning to any person responsible or in charge of the treatment when the operations

tions of treatment have violated the provisions of this Regulation;

d) order the person responsible or in charge of the treatment that the treatment operations be

comply with the provisions of this Regulation, where appropriate, of a given

manner and within a specified time;

The respondent does not adopt or plan to adopt any measure that tends to mitigate facts such as those examined.

Article 29.3 of Law 40/2015, on the Legal Regime of the Public Sector, in order to graduation of the sanctions provides: “In the normative determination of the sanctioning regime, as well as in the imposition of sanctions, the due suitability and necessity of the sanction to be imposed and its adequacy to the seriousness of the act constituting the infraction. The Graduation of the sanction will especially consider the following criteria: a) The degree of guilt or the existence of intent. b) The continuity or persistence in the behavior offending c) The nature of the damage caused. d) Recidivism, by commission in the term of one year of more than one infraction of the same nature when it has been declared by firm resolution in administrative proceedings.”

Applicable to both infractions, in this case because the alleged offender is a local entity, the article 83.7 of the RGPD indicates:

“Without prejudice to the corrective powers of the control authorities under article 58, paragraph 2, each Member State may establish rules on whether it is possible, and in what measure, impose administrative fines on authorities and public bodies established in that Member State"

The Spanish legal system has chosen not to fine entities public, as indicated in article 77.1. c) and 2. 4. 5. and 6. of the LOPDDGG: “1. The regime established in this article will be applicable to the treatments that 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 commit any of the infractions referred to in articles 72 to 74 of this organic law, the competent data protection authority will issue a resolution sanctioning the

themselves with warning. The resolution will also establish the appropriate measures

adopt to stop the behavior or correct the effects of the infraction that had occurred.

task.

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 under the

this article.

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

Therefore, in accordance with the applicable legislation

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE OVIEDO CITY COUNCIL, with NIF P3304400I, for a

violation of articles 32 and 5.1.f) of the RGPD, in accordance with articles 83.4.a) and

83.5.a) a warning sanction.

SECOND: NOTIFY this resolution to the OVIEDO CITY COUNCIL.

THIRD: In accordance with article 58.2.d) of the RGPD: “each control authority may order the person in charge or in charge of the treatment that the treatment operations be comply with the provisions of this Regulation, where appropriate, of a given manner and within a specified period…” the respondent is ordered to enter into function of the treatment risks derived from police action and the rights affected, the appropriate measures for the treatment of data with devices such as personnel policy in the performance of duties, granting him two months to report of the same carried out.

FOURTH:

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

COMMUNICATE this resolution to the OMBUDSMAN, of

In accordance with the provisions of article 50 of the LOPDGDD, this Resolution It will be made public once it has been notified to the interested parties.

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 Agency Spanish Data Protection Authority within a month from the day following the notification of this resolution or directly contentious-administrative appeal before the Chamber of the Contentious-administrative of the National High Court, in accordance with the provisions of the article 25 and in section 5 of the fourth additional provision of Law 29/1998, of 13 July, regulatory of the Contentious-administrative Jurisdiction, in the term of two months to count from the day following the notification of this act, as provided in 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, it may be precautionary suspension of the firm decision in administrative proceedings if the interested party expresses

its intention to file a contentious-administrative appeal. If this is the case, the

The interested party must formally communicate this fact in writing addressed to the Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Spanish Data Protection, presenting it through the Electronic Registry of the

Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through one of the

remaining records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1.

You must also transfer to the Agency the documentation that proves the effective filing

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

938-26102021

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es