 Procedure No.: PS/00420/2018

938-051119

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following

BACKGROUND

FIRST: On 09/06/2018 a claim is received from A.A.A. on behalf of B.B.B. (in

hereinafter the claimant), who works as a local police officer in ***LOCALIDAD.1, against the

CITY COUNCIL OF ***LOCALITY.1 (LOCAL POLICE) (hereinafter claimed).

He states that from the digital platform of his job, he has access to

by all the agents to all the data of the reports, both work and

any personal and health character. Without using any type of filter, you can view the

personal data of other officials, address, medical data, marital status. Although I do not know

can be modified, if it is accessed in reading mode, and there is no record of who accesses it.

Indicates that the platform contains a report disclosing your medical data

by one superior to another, the report being perfectly visible to any

co-worker.

Provides a copy of the impression of a screen obtained from the platform, "in the

job of another colleague" to "prove the ease with which anyone accesses

to the data", and your personal data is communicated between two superiors, data to which

any colleague can access it, without leaving a trace.

The screen contains a report with the title "Internal regime news"

shooting exercises not carried out by the PL XXX-shift leader with a number and name and

surnames and in Agents two numbers.

The commentary narrates the facts of a shooting exercise that policeman XXX did not

he was able to do, alluding that he had high blood pressure and that he would provide a medical report.

Noting that he met with the police officer to find out if it is a lasting issue or

transitory and exposing the motives and the lack of spirit of the police officer.

SECOND

requested to report:

: In view of the facts stated in the claim, it was transferred to the

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

1.

to the claim.

two.

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

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

Documentation proving that the claimant's right to be

3.

informed about the course and outcome of this claim.

It is verified that on 10/15/2018 the respondent received the document, and dated 11/26/2018,

response is received, indicating that the two reports have been sent to the claimant

They accompany in a letter of 11/19/2018.

a) The first, signed by a Chief Inspector, dated 11/2/2018, indicates on the claim-

tion that “The database to which the complainant alludes is a database of an in-

terno, which can only be accessed by using a username and password, accrediting

that access is only made by police components, which have the duty of secrecy,

keep professional secrecy". It distinguishes between processing for administrative purposes from those for

police investigation. Adds the obligation for officials to observe secrecy over

matters that they know and manifest only accessed the database police components-

them, concluding that there has been no disclosure of secrets, lack of professional secrecy or violation

secrecy, and that no action is required considering that the data

They are protected.

The second, from the Telecommunications and Information Technology Service, dated 10/30/2018, indicates

that access to the active directory is made with username and password. "The application

"Reports and reports of the Local Police was developed by the staff and the police service.

City Council computer. Its purpose is to collect all the actions carried out by

the agents of the headquarters with an indication, among others, of filling in the "report" field

which is freely drafted by each drafting agent. Once completed, it is included in a

supervision circuit that begins with the shift manager and ends with the supervision of

the senior staff and its subsequent archive. It indicates that "all the reports had to be

reading shares for all agents".

Regarding the "Agents application" it is developed as an auxiliary table of other

so many applications, in order to be able to record service shifts, list of agents

acting-reports and attestations, productivities made, noting that "all the

agents have access to the data of the same in equal conditions, in read only

without there being parts of it that are accessible in a restricted way by the senior staff"

An agreement to process the claim is issued on 12/4/2018.

THIRD: On February 6 and 7, 2019, written documents are received from the claimant's representative

indicating that a letter has been received from the Local Police, but not from the Protection Delegate

of Data, and that the answer does not correspond to "the facts denounced". accompanies

the Police brief, dated 11/19/2018, in which it is indicated that they are accompanied by a report from the

Chief Inspector of 2/11/2018 and another of the person in charge of implementations of the Department of computing of 10/30/2018.

On 03/11/2019, a letter was received from the claimant indicating that he had not received communication of the agreement reached regarding your claim.

FOURTH: On 07/12/2019, the Director of the AEPD, initiated a procedure of warning against the CITY COUNCIL OF ***LOCALITY.1 (LOCAL POLICE) for alleged infringement of article 5.1.f) of Regulation (EU) 2016/679 of the Parliament European and Council of 04/27/2016 regarding the protection of natural persons in the regarding the processing of personal data and the free circulation of these data (as far hereinafter, RGPD), for an infringement that is included in article 83.5.a) of the RGPD, as stated in article 58.2.b) of the RGPD in relation to article 77.2 of the Law Organic 3/2018, of 5/12, on the Protection of Personal Data and guarantee of rights (hereinafter LOPDGDD).

FIFTH: On 08/02/2019, the respondent indicates in her allegations:

a) Report issued by the Accidental Chief Inspector of Administrative Services that in synthesis indicates:

-The start-up agreement was transferred to the information technology area, which communicates that "there have been carried out the corrective measures to avoid the incidence to which it makes reference the file, carrying out the creation of a computer application specific for the preparation of personal reports and internal regime related to

Agents, guaranteeing data security and protection.”

The application is restricted to the shift manager who writes the report, the

Taxable agent of the same, and the member of the senior staff to whom the

report.

Only the managers of the Headquarters can access the application to create

reports.

Agents are advised not to use the above application”

reports and

” for the preparation of writings on the internal regime or personal reports.

crowded

Letter from the “responsible for implementations of the IT area”, dated 07/29/2019

b)

which indicates the same thing.

c)

Reiterates the sending of the letter from the Local Police Chief Inspector of 11/2/2018.

Provide a copy of a document addressed to the claimant, reference YYYYY-2018 of

d)

11/8/2018 in which it appears that they send reports from 11/2/2018 and another from Informatica de

10/30/2018.

SIXTH: On 02/10/2020, a resolution proposal was issued for the literal:

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

with a warning to the CITY COUNCIL OF *** LOCALITY.1 (LOCAL POLICE), for a

infringement of Article 5.1.f) of the RGPD, in accordance with article 83.5 of the RGPD.”

SEVENTH: Against the proposal no arguments were received.

PROVEN FACTS

The claimant works as a local police officer in ***LOCATION.1. The performance of your

1)

job is done in part through a computer application. The application

allows you to enter information and data on the professional actions of each Agent.

The claimant provides a printed copy of a screenshot obtained from the

two)

computer platform with which it works, tab "INTERNAL REGIME" which reads:

“New internal regime” “shooting exercises not carried out by PL XXX” “shift leader”

with your number and name and surname and in the "Agents" field two agent numbers, one

that of the shift manager. The commentary narrates the events that occurred “on the occasion of the

routine shooting practices that are being carried out by the components of the squad, the

police officer PL-RRR (shooting instructor) informs me that...”, he refers to the target practice of

which the claimant police officer identified by his number XXX was part of. It is informed

who has not done the internship for more than a year and "always alleges medical problems" that

"He told me that he had high blood pressure and that he would provide a medical report." It is also indicated

also that he met with the police to find out if it is a lasting or transitory matter

and exposing the motives and the lack of spirit of the policeman.

3)

The respondent indicates in pleadings to the agreement that the content of the writing has changed.

INTERNAL REGIME, so that it has limited the users who can write, in-

browse and read these writings. A specific application has been created for this.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of

control, and as established in arts. 47 and 48.1 of the LOPDGDD, the Director of the

Spanish Agency for Data Protection is competent to resolve this procedure.

II

In the STC 292/2000, of 11/30, the object and content of the right to

data protection in the terms set out below.

The fundamental right to data protection, enshrined in article 18.4 of the

Spanish Constitution, unlike the right to privacy of art. 18.1 EC, with whom

shares the objective of offering an effective constitutional protection of private life

personal and family, excluding the knowledge of others and the interference of third parties in

against their will, seeks to guarantee that person a power of control over their data

about their use and destination, with the purpose of preventing their illicit and harmful traffic to

the dignity and rights of the affected.

The right to data protection has, therefore, a broader object than that of

right to privacy, since the fundamental right to data protection extends its

guarantee not only to privacy in its dimension constitutionally protected by art. 18.1

CE, but to the sphere of the goods of the personality that belong to the sphere of life

privacy, inseparably linked to respect for personal dignity, such as the right to

honor, and to the full exercise of the rights of the person. The fundamental right to

data protection extends the constitutional guarantee to those data that are

relevant or have an impact on the exercise of any rights of the person, whether or no constitutional rights and whether or not related to honor, ideology, personal privacy and familiar to any other constitutionally protected property.

In this way, the object of the fundamental right to data protection is not reduced only to the intimate data of the person, but to any type of personal data, whether or not intimate, whose knowledge or use by third parties may affect their rights, whether or not fundamental - such as those that identify or allow the identification of the person, being able to serve for the preparation of their ideological, racial, sexual, economic or any other nature, or that serve for any other use that in certain circumstances constitutes a threat to the individual, because its object is not only the individual privacy, already protected by art. 18.1 CE, but personal data. By Consequently, it also reaches those public personal data, which due to the fact of be, if they are accessible to the knowledge of anyone, they do not escape the power of disposition of the affected party because this is guaranteed by their right to data protection.

Regarding its content, the fundamental right to data protection attributes to its holder a bundle of faculties consisting of various legal powers whose exercise imposes legal duties on third parties, which are not contained in the fundamental right to privacy, and that serve the capital function that this fundamental right performs: guarantee the person a power of control over their personal data, which is only possible and effective imposing on third parties the aforementioned duties to do. Among them, highlight the right to require prior consent for the collection and use of personal data. personal data, the right to know and be informed about the destination and use of such data and the right to access, rectify and cancel said data. This ensures the power disposition of personal data

In the development of labor provision, civil servants like any other employee have the right to the protection of their data, since the statutory relationship does not

except the configuration of this right, nor can it be considered as a title

legitimizer of cuts in the exercise of the fundamental rights that concern the

worker as a citizen, who does not lose his condition as such by inserting himself in the sphere of

an organization (STC 99/1994).

In this case, the comments made on the occasion of the holding of an exercise

claimant's shooting range with his instructor, which contained references to health issues,

psychological and service do not concern third parties, including among these their colleagues,

that although they are police officers and are subject to the duty of secrecy, this does not mean that it cannot be denied

who have been able to learn about the circumstances associated with the claimant, and whose purpose was not

is.

The facts should have been kept in the chain of ordinary management of

matters between the parties, without the possibility of employee access,

producing a revelation of the facts and a violation of their privacy.

III

The defendant is accused of committing an infringement of article 5.1 f) of the RGPD

That points:

“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 principle of data security imposes the obligation to adopt the measures
of a technical and organizational nature that guarantee that, adding that such measures have
with the purpose of avoiding and guaranteeing that, among other aspects, by way of example,
produces an "unauthorized access" by third parties, or that third parties, not interested,
by the configuration of the application as it happens in this case they can read writings
referred to the internal management of personnel matters or internal regime. The management of
risk that the information that is associated with the personal data is not known by
those not affected or interested has failed in the development of the computer application of the
claimed, which from its design has to count on safeguarding said end so that
their confidentiality is not violated, without it being enough to adopt
any measure, since they must be those necessary to guarantee those objectives that
mark the rule. In addition, everyone responsible for a file must ensure that said
measures or mechanisms are implemented effectively in practice being
responsible that they are complied with and executed rigorously, having to carry out
periodic performance evaluations.
The GDPR broadly defines “data security breaches”.
personal” as “all those violations of security that cause the destruction,
accidental or unlawful loss or alteration of personal data transmitted, stored or
otherwise processed, or unauthorized communication or access to said data.” The
Security incidents must be notified to the AEPD when they constitute a risk for the
rights and freedoms of natural persons, and in this case that risk has materialized
with the provision of data to third parties, even if they were from the same group and in the circle
of police officers who manage the database and provide services at the headquarters of the requested party.
In the present case, the commission of the infraction that is given to the power
employees view the content of internal reports that are processed in management of
personnel on the obligations of the police components. In this sense, emphasis should be placed

that although the accesses are carried out using a password and username, it was not an obstacle to

that by the configuration of the accesses, each one could freely access this

report.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Article 83.7 of the RGPD indicates:

III

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

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

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

established in that Member State.

Article 58.2 of the RGPD provides the following: "Each supervisory authority

shall have all of the following corrective powers listed below:

a)

sanction any person responsible or in charge of the treatment with a warning

when the treatment operations have violated the provisions of this

Regulation;

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

treatment comply with the provisions of this Regulation, where appropriate, in accordance with

a certain way and within a specified period;

Article 72.1.a) of the LOPDGDD indicates: “Infringements considered very serious

"1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679,

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

substantial violation of the articles mentioned therein and, in particular, the

following:

The processing of personal data violating the principles and guarantees

a)

established in article 5 of Regulation (EU) 2016/679".

Adding article 77.2 of the LOPGDD:

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

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

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

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

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

would have committed

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

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

interested, if any.

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

data 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

proves the existence of technical reports or recommendations for treatment that are not

had been duly attended to, in the resolution in which the sanction is imposed,

will include a reprimand with the name of the responsible position and order the

publication in the corresponding Official State or Autonomous Gazette.

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

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

previous.

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

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

protection of this article.

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

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

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

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

When the competence corresponds to a regional data protection authority

it will be, in terms of the publicity of these resolutions, to what its regulations have

specific."

In this sense, there is a change in the way of managing the reports of

internal regime of the local police.

Therefore, in accordance with the applicable legislation,

the Director of the Spanish Data Protection Agency RESOLVES:

TOWN HALL OF

FIRST: IMPOSE a sanction of WARNING on the

***LOCALIDAD.1 (LOCAL POLICE), with NIF P1103100B, for a violation of Article

5.1.f) of the RGPD, in accordance with article 83.5 of the RGPD.

SECOND: NOTIFY this resolution to the CITY COUNCIL OF ***LOCALITY.1

(LOCAL POLICE).

THIRD

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

: COMMUNICATE this resolution to the OMBUDSMAN, of

FOURTH: In accordance with the provisions of article 50 of the LOPDGDD, this

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

following the notification of this resolution or directly contentious appeal

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

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

of Law 29/1998, of 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 pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP,

may provisionally suspend the firm resolution in administrative proceedings if the interested party

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

In this case, the interested party must formally communicate this fact in writing addressed to the

Spanish Agency for Data Protection, presenting it through the Electronic Registry

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

effectiveness of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within two months from the day

following the notification of this resolution, it would end the suspension

precautionary

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es