 File No.: PS/00596/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: On January 7, 2021, D. A.A.A. (hereinafter, the complaining party),

filed a claim with the Spanish Agency for Data Protection against the

CITY COUNCIL OF OURENSE, with NIF P3205500F (hereinafter, the

claimed).

The grounds on which the claim is based are as follows:

On January 5, around 10 p.m., in Ourense, on ***DIRIMIENTO.1 street, the

Agent nº***AGENTE.1 of the Local Police, requested the DNI for identification. In

moment of having it in his hand, he photographed it without his consent and without clarifying the

use to be made of said data. Due to this defenseless situation and the

device used by the Agent, considers that the security of the

your personal data and photo of the DNI, for which you request that said image be

eliminated, since said Agent has no reason to use and store it.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, of Protection of Personal Data and guarantee of digital rights (in

hereinafter LOPDGDD), said claim was transferred to the claimed party, to

to proceed with its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements set forth in the regulations of

Data Protection.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

(hereinafter, LPACAP), by electronic notification, was received in

date March 1, 2021, as stated in the certificate in the file.

No response has been received to this transfer letter.

THIRD: On May 12, 2021, in accordance with article 65 of the

LOPDGDD, the claim filed by the claimant was admitted for processing.

FOURTH: The General Subdirectorate for Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts in

matter, by virtue of the investigative powers granted to the authorities of

control in article 57.1 of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter RGPD), and in accordance with the provisions of the

Title VII, Chapter I, Second Section, of the LOPDGDD, having knowledge of the

following ends:

On May 26, 2021, the Data Inspection requested the City Council

of Ourense, so that, within a period of ten days, it could provide certain information and

documentation in order to clarify the reported facts.

On July 7, 2021, a written response to said document was received.

requirement in which, in summary, the following is stated:

Regarding the legality of the processing of personal data by the Local Police to

when requesting the data of a citizen and that they do so by carrying out

from a photograph to your National Identity Document:

They state that the General Data Protection Regulation (RGPD) designs a

system of legitimation based on six legal bases that do not maintain each other

no relationship of priority or precedence.

In particular, and for the scope of the Local Administration, the

following:

The treatment is necessary for the fulfillment of a legal obligation

•

applicable to the data controller.

•

Processing is necessary for the fulfillment of a mission

carried out in the public interest or in the exercise of public powers vested in the

responsible for the treatment.

In this case, they allege the following:

-

The State Security Forces and Bodies are

fully authorized to request or take the data of people with

investigative, preventive reasons or for those cases that occur

in the context that the individual may be incurring in some type of

illegality or violation of the law, all in accordance with the provisions of the

Organic Law 3/2018, of December 5, on the Protection of Personal Data and

Guarantee of Digital Rights, the European Directive 2016/680, of 27

April 2016, on the protection of natural persons with regard to

to the processing of personal data by the competent authorities

for purposes of prevention, investigation, detection or prosecution of

criminal offenses or the execution of criminal sanctions, and the free

circulation of such data and the General Data Protection Regulation,

of same date.

-

Organic Law 4/2015, of March 30, on Security Protection

Citizen, establishes in articles 16.1 and 9.2 that citizens must

obligatorily to present your personal data or DNI when the agents of

the Security Forces and Bodies require their identification in the

following situations:

a) When there are indications that they may have participated in the commission of

an infraction.

b) When, in view of the concurrent circumstances, it is considered

reasonably necessary to prove your identity to prevent the

commission of a crime.

-

At the moment in which an agent of the authority takes photographs

of an identity document, it is necessary to place said document in a legal context.

procedure, taking into account that the regulations imposed

for those who deal with the processing of personal data of a

individual. Thus, in the Organic Law 3/2018 that deals with the Guarantees of

Digital Rights and the Protection of Personal Data establishes that the

agent that carries out the treatment of the personal information of

citizens must guarantee that said procedure complies with the measures

of confidentiality and security established for the protection of data and

personal information. Therefore, in accordance with the foregoing, the Agents of the FyCSE understand that they may process personal data when requested to identification purposes. Still, when an agent takes a picture of the DNI, we must focus on the scope of compliance with the measures security that the data protection regulations require from the person responsible for the treatment.

-

The LO 3/2018 of Protection of Personal Data and Guarantee of digital rights, requires data controllers to adopt the corresponding security measures of a technical and organizational nature necessary to guarantee that the treatment is in accordance with the regulations valid. In other words, taking a citizen's affiliation data for their subsequent treatment must be carried out with methods that guarantee the safety and confidentiality of personal data. In the event that the agents use particular devices for taking images of the data personal data contained in the DNI in the exercise of its functions does not guarantee totally the security of the data, since the private use of each agent can make your device would not be compatible with the measures of security that for the exercise of the functions of inquiry, investigation and prevention of crimes and infractions must be adopted. In addition, it is appropriate point out that said device is out of the control of the person in charge of the treatment.

-

A different question will be whether the device through which the image belongs to the organization, instead of being personal, it is corporate, being susceptible that the policies and measures of

control and security that guarantee that said treatment is carried out in accordance with

data protection regulations.

In relation to the claim presented by the claimant in which he states that

a Local Police Agent asked for his identification and photographed him with a cell phone without

your consent the DNI, for which you request the deletion of the images taken,

they state:

They state that the city council has reviewed procedures carried out

-

carried out by the Police Headquarters in order to know the scope and

procedures for the use of mobile devices.

(...).

-

-

The Police Headquarters has drawn up a user manual for the

Incorporation of images to the files. The training emphasized

that all the photographs must be taken with the provided terminal,

Official instructions on proper use are pending and under development.

-

They allege that it is considered adjusted to law and to the regulations in force

Regarding the treatment and protection of personal data, the use of

corporate devices by the Local Police of Orense with and for the

described purpose.

Regarding the request to remove the image of the DNI taken by the agent:

-

Regarding the treatment of the photographs taken, they state that

These will be eliminated once the purpose for which they were has concluded.

taken, that is, opening of file, which as of today is

still in process.

-

They state that since the file is still in progress, they were

notify D.A.A.A. the circumstance in which your treatment is located

personal information.

Regarding the information provided to the claimant regarding the processing of data

of a personal nature collected:

There is no evidence that information was provided to the claimant in the

-

terms provided in art. 13 of the GDPR.

On September 9, 2021, the Data Inspection requested the

Orense City Council information and documentation in order to clarify the

legal context and the scope (criminal or administrative) in which the action is framed

of the Police Agent.

On October 18, 2021, he received a written response to the request

in which they show that, in the case at hand, it is an act of

complaint for skipping the curfew established by the pandemic situation and

They attach a screenshot, which shows the beginning of the sanctioning file

in the Subdelegation, which informed them to refer him to the Xunta since it was the

competent to sanction these matters.

On October 26, 2021, the Data Inspection requested the

City Council of Orense, in relation to the photograph taken by the Local Police of the

identity document of A.A.A., clarification on whether said photograph was taken with

a corporate mobile terminal, or another device outside the City Council was used.

On November 25, 2021, he had a written reply to the

requirement in which they show the following:

The photograph was taken by a device other than the corporate ones.

Since March 16, 2021, the Ourense Local Police uses in

-

-

their performances, corporate devices.

-

Incorporation of images to the files.

-

once the purpose for which it was taken has ended.

As for the photograph obtained, it was deleted from the device

The Police Headquarters has drawn up a user manual for the

FIFTH: On April 5, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimed party,

for the alleged infringements of articles 5.1.c) and 32 of the RGPD, typified in the

articles 83.5 and 83.4 of the RGPD, respectively.

The initiation agreement was sent, in accordance with the regulations established in the Law

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

Public Administrations (hereinafter, LPACAP), by electronic notification,

being received on April 5, 2022, as stated in the certificate that is in

The file.

SIXTH: After the term granted for the formulation of allegations to the agreement

of the beginning of the procedure, it has been verified that no allegation has been received

by the claimed party.

Article 64.2.f) of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (hereinafter LPACAP) -provision of which

the party claimed was informed in the agreement to open the proceeding-

establishes that if allegations are not made within the stipulated period on the content of the

initiation agreement, when it contains a precise statement about the

imputed responsibility, may be considered a resolution proposal. In the

present case, the agreement to initiate the disciplinary proceedings determined the

facts in which the imputation was specified, the infraction of the RGPD attributed to the

claimed and the sanction that could be imposed. Therefore, taking into account that

the party complained against has made no objections to the agreement to initiate the file and

In accordance with the provisions of article 64.2.f) of the LPACAP, the aforementioned agreement of

beginning is considered in the present case resolution proposal.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: It is recorded that on January 7, 2021, the complaining party filed

claim before the Spanish Agency for Data Protection, whenever a

Agent of the Local Police photographed his DNI for his identification, without his

consent.

SECOND: The photograph was taken by a device other than the corporate ones of the

Local police.

THIRD: The photograph was taken in the context of the identification of the claimant-

in the verification of a possible infraction such as skipping the curfew

established by the pandemic situation.

FOURTH: In relation to the treatment of the DNI photograph, the respondent affirms

that will be eliminated “once the purpose for which they were taken is over, that is,

cir, opening of file”, which, on the date of formulation of that allegation, was

smuggling still in process.

FOUNDATIONS OF LAW

FIRST: In accordance with the powers that article 58.2 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter RGPD), grants

each control authority and as established in articles 47 and 48.1 of the Law

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

digital rights (hereinafter, LOPDGDD), is competent to initiate and resolve

this procedure the Director of the Spanish Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that: “The procedures

processed by the Spanish Agency for Data Protection will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures."

SECOND: As established in section III of the "Preamble" of the Organic Law 4/2015, of March 30, on the protection of citizen security (LOPSC), "(...) empowers the competent authorities to agree on different actions aimed at maintenance and, where appropriate, the restoration of citizen tranquility in assumptions of public insecurity, regulating with precision the budgets, the and the requirements to carry out these procedures, in accordance with the principles, among others, of proportionality, minimal interference and non-discrimination (...)".

And so they are established in articles 9.2 and 16.1 of the LOPSC, regarding the obligation to display and allow verification of the DNI by agents of the Forces and State Security Corps.

In article 9, on the obligations and rights of the holder of the National Document of Identity, indicates that:

"two. All persons required to obtain the National Identity Document they are also to exhibit it and allow the verification of the security measures to those referred to in section 2 of article 8 when required to do so by the authority or its agents, for the fulfillment of the purposes set forth in section 1 of article 16. You must report your theft or loss as soon as possible. possible to the nearest Police station or post of the Security Forces and Bodies next".

In its article 16, on the Identification of people, it is established that:

1. In the fulfillment of its functions of criminal investigation and prevention, as well as for the sanction of penal and administrative infractions, the agents of the Forces and Security Bodies may require the identification of the persons in the following assumptions:

a) When there are indications that they may have participated in the commission of a

infringement.

b) When, in view of the concurrent circumstances, it is considered

reasonably necessary to prove your identity to prevent the commission of a

crime. In these cases, the agents may carry out the checks

necessary on public roads or in the place where the request was made,

including the identification of persons whose face is not fully or partially visible

for using any type of garment or object that covers it, preventing or hindering the

identification, when necessary for the indicated purposes.

In the practice of identification, the principles of

proportionality, equal treatment and non-discrimination based on birth,

nationality, racial or ethnic origin, sex, religion or belief, age, disability,

sexual orientation or identity, opinion or any other condition or circumstance

personal or social.

Therefore, the State Security Forces and Bodies can process the data

of citizens for the prevention, investigation, detection or

prosecution of criminal offenses and for the performance of the functions of

public interest that are their own. However, these treatments must be

carried out respecting at all times, what is established in the regulations in force in

matter of protection of personal data, the RGPD and the LOPDGDD,

respectively.

THIRD: Regarding the application of data protection regulations

to the assumption raised, it must be taken into account that the RGPD, in its article 32, requires to those responsible for the treatment, the adoption of the corresponding measures of security necessary to guarantee that the treatment is in accordance with the regulations in force, as well as to guarantee that any person acting under the authority of the responsible or of the person in charge and has access to personal data, can only treat them following the instructions of the person in charge.

Article 32 of the RGPD, security of treatment, establishes the following:

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

a) pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and evaluation of the effectiveness of the technical and organizational measures to guarantee the security of the treatment.

2. When evaluating the adequacy of the security level, particular consideration shall be given to taking into account the risks presented by the processing of data, in particular as consequence of the accidental or unlawful destruction, loss or alteration of data data transmitted, stored or otherwise processed, or the communication or unauthorized access to said data (The underlining is from the AEPD).

On the other hand, Recital (74), of the RGPD indicates that: "It must be established

the responsibility of the data controller for any data processing

personal made by himself or on his behalf. In particular, the controller must

be obliged to apply timely and effective measures and must be able to demonstrate the

compliance of processing activities with this Regulation, including the

effectiveness of the measures. Such 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.

Thus, the taking of the personal identification data of a citizen, by

Police officers, must be carried out with methods that guarantee the safety and

confidentiality of these, following the instructions of the data controller.

In the present case, the claimant denounces that when he showed the DNI, the Agent

took a photograph of the document with a mobile phone, thus exceeding the limits of the

rights that assist him, while, for his part, the claimed party states that

the photograph was taken with a device other than the corporate ones.

Therefore, it should be examined whether such home cameras and mobile phones can

guarantee the security of the data in such a way that there is no loss or

data alterations and, especially, given the widespread use of

smart devices, the possibility of access by third parties to the data on them

stored. It should thus be taken into account that an inadvertent

transfer of data to third parties.

Taking into account the risks indicated, it should be considered that the use of cameras or

personal mobile phones of the agents does not guarantee the security of the data, while

the private uses that each agent can carry out with their own devices are not

are compatible with the security measures that for the exercise of the

police functions must be adopted by those responsible for the police file of which

such recordings will be part.

Also, in the event that smart devices are used that have been

delivered officially for use with police purposes, they must

respond to regulatory requirements, in particular, adopting all the

precautions to prevent improper access to the data that is captured with them.

In the specific case under examination, the action carried out through the mobile phone

different from the corporate ones for collecting data from the claimant constitutes an infringement of

the provisions of article 32 of the RGPD, typified in article 83.4 of the RGPD.

Article 83.4.a) of the aforementioned RGPD establishes the following:

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

paragraph 2, with administrative fines of a maximum of EUR 10,000,000 or,

in the case of a company, an amount equivalent to a maximum of 2% of the

global total annual turnover of the previous financial year, opting for

the largest amount:

a)

the obligations of the person in charge and the person in charge in accordance with articles 8,

11, 25 to 39, 42 and 43."

(…)

For the purposes of the limitation period for infractions, article 73 of the LOPDGDD, under the heading "Infringements considered serious", it establishes the following:

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

(…)

f) The lack of adoption of those technical and organizational measures that result 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.

In the present case, the infringing circumstances provided for in article 83.4 of the GDPR, transcribed above.

FOURTH: Article 5 of the RGPD establishes the principles related to the processing of personal data by the person responsible and/or in charge of the same and in section 1.c) it is specified that: "personal data will be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization").

It should be clarified that this article does not limit the excess of data, but the need. It is In other words, the personal data will be "adequate, pertinent and limited to the need", for which they were collected, in such a way that it must be evaluated if the objective persecuted could have been reached by other means, without carrying out a treatment excessive data, as in our case. This is also established by the Recital 39 of the RGPD, when it indicates that: "Personal data should only be processed if the purpose of the treatment could not reasonably be achieved by other means.

Therefore, only the data that is adequate, pertinent and not

excessive in relation to the purpose for which they are obtained or processed. The categories of

Data selected for processing must be strictly necessary to

achieve the stated objective and the controller must strictly limit

the collection of data to that information that is directly related to the

specific goal to be achieved.

In the case examined, the treatment consisted of taking the photograph

identity card through the personal cell phone of the police officer, as well as its conservation, until the

opening of the administrative file. This treatment is clearly excessive,

noting that the principle of "data minimization" also imposes the suppression

sion of the image immediately after the aforementioned

ID.

For these purposes, it is necessary to point out that the purpose alleged by the respondent for the

maintenance of the photograph would be the “dump in the application for the opening of the

proceedings". In other words, there is not even an alleged purpose of including the

document in the file itself, which in any case should be motivated. With that,

there is even less justification for preserving the image, which is

devoid of any purpose.

For all these reasons, the action in this case of the defendant supposes the violation of the

principle of "data minimization", contained in the aforementioned article 5.1.c) RGPD, where

It is established that the processing of personal data must be “adequate,

relevant and limited to what is necessary in relation to the purposes for which they are

treaties", typified in article 83.5 of the RGPD.

Article 83.5 of the RGPD provides the following:

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

paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or,

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

global total annual turnover of the previous financial year, opting for

the largest amount:

a)

basic principles for treatment, including conditions for con-

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

For its part, article 71 of the LOPDGDD, under the heading "Infringements" determines what

following: Violations constitute the acts and conducts referred to in the

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.

For the purposes of the limitation period for infractions, article 72 of the LOPDGDD,

under the rubric of infractions considered very serious, it establishes the following: "1. In

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:

a) The processing of personal data violating the principles and guarantees

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

In the present case, the infringing circumstances provided for in article

83.5 of the GDPR, transcribed above.

FIFTH: Establishes Law 40/2015, of October 1, on the Legal Regime of the Sector

Public, in Chapter III on the "Principles of the power to sanction", in the

Article 28 under the heading "Responsibility", the following:

"1. They may only be sanctioned for acts constituting an administrative infraction.

natural and legal persons, as well as, when a Law recognizes their capacity to

to act, the affected groups, the unions and entities without legal personality and the

independent or autonomous estates, which are responsible for them

title of fraud or guilt."

Lack of diligence in implementing appropriate security measures

constitutes the element of guilt.

SIXTH: Article 83 "General conditions for the imposition of fines

administrative "of the RGPD in its section 7 establishes:

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

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

can, and to what extent, impose administrative fines on authorities and organizations

public authorities established in that Member State."

The Spanish legal system has chosen not to fine entities

public but with a warning, as indicated in article 77.1. c) and 2. 4. 5. and 6.

of the LOPDGDD:

"1. The regime established in this article will be applicable to the treatment of

who are responsible or in charge:

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

autonomous and the entities that make up the Local Administration."

2. When those responsible or in charge listed in section 1 committed
any of the infractions referred to in articles 72 to 74 of this law
organic, the data protection authority that is competent will dictate
resolution sanctioning them with a warning. The resolution will establish
also the measures that should be adopted to stop the behavior or correct it.
the effects of the infraction that had been committed.
The resolution will be notified to the person in charge or in charge of the treatment, to the body of the
that depends hierarchically, where appropriate, and to those affected who had the condition
interested party, 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
sufficient evidence for it. In this case, the procedure and the sanctions to be applied
will be those established in the legislation on disciplinary or sanctioning regime that
result of application.
Likewise, when the infractions are attributable to authorities and managers, and
proves the existence of technical reports or recommendations for the treatment that
had not been duly attended to, in the resolution imposing the
The sanction will include a reprimand with the name of the responsible position and
will order the publication in the Official State or Autonomous Gazette that
correspond.
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 similar institutions
of the autonomous communities the actions carried out and the resolutions issued
under 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 person in charge or in charge of the treatment that had committed the infraction.
When the competence corresponds to a regional authority for the protection of
data will be, in terms of the publicity of these resolutions, to what your
specific regulations."

In accordance with these criteria, it is considered appropriate to sanction with a warning the
claimed party, for infringement of article 5.1.c) of the RGPD, when carrying out a treatment
excessive use of personal data in relation to the purpose for which it was being
collecting, and for the infringement of article 32 of the RGPD, considering that the
Taking a photograph of the claimant's DNI with a non-corporate mobile phone
it is an act that does not guarantee a level of security appropriate to the risk of the treatment
of personal data.

SEVENTH: Article 58.2 of the RGPD provides: "Each control authority will have
of all the following corrective powers indicated below:

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 a specified manner and within a specified period;"

Likewise, it is appropriate to impose the corrective measure described in article 58.2.d) of the
RGPD and order the claimed party to establish the appropriate security measures.

so that the treatments are adapted to the requirements contemplated in the

articles 5.1.c) and 32 of the RGPD, preventing situations such as the one that

has given rise to the claim.

The text of the resolution establishes the infractions committed and

the facts that have given rise to the violation of the regulations for the protection of

data, from which it is clearly inferred what measures to adopt, without prejudice

that the type of specific procedures, mechanisms or instruments for

implement them corresponds to the sanctioned party, since it is responsible for the

treatment who fully knows your organization and has to decide, based on the

proactive responsibility and risk approach, how to comply with the RGPD and the

LOPDGDD.

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of the sanctions whose existence has been proven, the Director of the

Spanish Data Protection Agency RESOLVES:

FIRST: SANCTION with a WARNING the CITY COUNCIL OF OURENSE,

with NIF P3205500F, for an infringement of article 5.1.c) of the RGPD, typified in the

article 83.5 of the RGPD.

SANCTION with a WARNING to the CITY COUNCIL OF

SECOND:

OURENSE, with NIF P3205500F, for an infringement of article 32 of the RGPD,

typified in article 83.4 of the RGPD.

THIRD: REQUEST the CITY COUNCIL OF OURENSE to implement the

necessary corrective measures to adapt their actions to the regulations of

protection of personal data, which prevent events from being repeated in the future

Similar.

FOURTH: NOTIFY this resolution to the CITY COUNCIL OF OURENSE.

FIFTH: COMMUNICATE this resolution to the Ombudsman, in accordance

with the provisions of article 77.5 of the LOPDGDD.

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 month from

counting from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the

National Court, 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 a period of two months 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,

may provisionally suspend the firm resolution in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registers provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the documentation proving the effective filing of the contentious appeal-administrative. If the Agency was not aware of the filing of the appeal contentious-administrative within a period of two months from the day following the notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-100322

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es