 Procedure No.: PS/00463/2019

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following:

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claimant) on 10/17/2018 filed

claim before the Spanish Data Protection Agency. The claim is

directed against BAENA CITY COUNCIL, with NIF P1400700I (hereinafter, the

claimed or TOWN HALL). The grounds on which the claim is based are

statements of the complainant, in short: that when checking in the electronic office

of the claimed, through the secure verification code (CSV), the collective certificate

of registration that his father had requested, the system of the electronic headquarters

returns 23 certificates of various kinds related to the register where they appear

personal data of the components of the family of the claimant and of the interested parties

of the other 22 certificates signed on the same day. All certificates signed on

same day have the same CSV. The claimant requests that since it cannot be

change the CSV after it is generated, an additional field is entered into the system, or

second step where the DNI is requested to be able to discriminate the correct document

before viewing it.

SECOND: In view of the facts denounced in the claim and the

documents provided by the claimant, the Subdirectorate General for Inspection of

Data proceeded to carry out preliminary investigation actions for the

clarification of the facts in question, by virtue of the investigative powers

granted to the control authorities in article 57.1 of the Regulation (EU)

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

in accordance with the provisions of Title VII, Chapter I, Second Section, of the Law Organic 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter LOPDGDD).

On 07/23/2019, the claimant is requested to specify the CSV and the documents you refer to in your claim.

On 07/29/2019, this Agency received a letter sent by the claimant providing the requested information.

And attach the following documentation:

• Collective Register Registration Certificate corresponding to the family of the claimant

• The 23 documents shown in the electronic office of the CITY COUNCIL at enter as verification code the one corresponding to the certificate of the claimant.

The background information is the following:

With the notification date of 12/13/2018, the claim is transferred to the CITY COUNCIL requesting the following information: (i) copy of the communications, of the decision adopted that has been sent to the claimant regarding the transfer of this claim, and proof that the claimant has received the communication of that decision, (ii) report on the causes that have motivated the incidence that has originated the claim, (iii) report on the measures adopted to prevent the produce similar incidents and (iv) any other that it considers relevant.

Dated 02/13/2019, without having received in this Agency the information

requested in the transfer of the claim, it is agreed to admit the claim for processing

filed by the claimant against the TOWN HALL.

Despite the fact that the CITY HALL has been informed through the transfer of the

claim of the incident detected, still continues to expose the personal data of

the interested parties that appear in the 23 documents of the register that are obtained at the

enter the CSV of the collective registration certificate.

THIRD: On 02/07/2020, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged

infringement of articles 32.1, 33 and 34 of the RGPD, sanctioned in accordance with the

provided in article 83.4.a) of the aforementioned RGPD.

FOURTH: Notification of the aforementioned initiation agreement, in writing of 03/06/2020, the claimed

stated that it was true that in the issuance of the certificate indicated by the claimant,

included by mistake other certificates made that day and that were

digitized together; that in relation to said incident by the Technician

computer, a report was issued on the causes that motivated the same and that

gave rise to the claim and the measures taken to prevent the occurrence

similar facts; that by the Head of the Bureau of the Citizen Attention Service

where said certificates are issued issued a report from which it can be deduced that in the

Currently, these certificates, whatever their class, are issued in a

individualized and automated through GEX.

SIXTH: On 06/02/2020, a Resolution Proposal was issued in the sense of

that the defendant be sanctioned with a warning for violation of the articles

32.1, 33 and 34 of the RGPD, typified in article 83.4.a) of the aforementioned RGPD and

sanctioned in accordance with the provisions of article 77.2 of the LOPDGDD.

After the period established for this purpose, the respondent has not submitted a written

allegations at the time of issuing this resolution.

SEVENTH: Of the actions carried out in this proceeding,

the following have been accredited,

PROVEN FACTS

FIRST. On 10/17/2018 there is an entry in the AEPD written by the claimant

stating that when checking in the electronic headquarters of the claimed, through the

secure verification code (CSV), the collective registration certificate that

his father had requested, the electronic office system returns 23 certificates of

various kinds related to the register where personal data of the

components of the claimant's family and the interested parties of the other 22

certificates signed the same day. All certificates signed on the same day have

the same CSV.

SECOND. It consists provided Collective Registration Certificate requested by

the father, in which the persons registered in the domicile appear.

THIRD. There are 23 documents provided by the claimant requested by

different persons and related to different types of certifications issued by the

Municipal Register of Inhabitants of the Baena City Council who share CSV and

date of issue: Collective, Individual, Historical Movement Certificates and

changes of data or register, new registrations, etc.). In the aforementioned documents are

personal data relating to registered persons: name and surname, place

and date of birth, DNI, address and registration date in the Register, etc.

FOURTH. The respondent has provided a technical report prepared by the person in charge Municipal informatics in which the causes that motivated the incident are analyzed as well as as the technical and corrective measures adopted to prevent the occurrence of similar events in the future.

It is also recorded that the Department of Citizen Attention was requested to issue a report on how to issue collective certificates of registration, noting that both the individual certificates and the collective and historical, individual and collective, issued from the Padrón of Inhabitants were made individually and automated through GEX.

FOUNDATIONS OF LAW

By virtue of the powers that article 58.2 of the RGPD recognizes to each control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD, The Director of the Spanish Agency for Data Protection is competent to initiate and to solve this procedure.

Yo

Article 58 of the RGPD, Powers, states:

"two. Each supervisory authority will have all of the following powers corrections listed below:

II

(…)

i) impose an administrative fine under article 83, in addition to or in instead of the measures mentioned in this paragraph, depending on the circumstances of each particular case;

(…)"

The RGPD establishes in article 5 of the principles that must govern the treatment of personal data and mentions among them that of "integrity and

confidentiality”.

The article notes that:

"1. The personal data will be:

(…)

f) treated in such a way as to ensure adequate security of the

personal data, including protection against unauthorized or unlawful processing and

against its loss, destruction or accidental damage, through the application of measures

appropriate technical or organizational ("integrity and confidentiality").

In turn, the security of personal data is regulated in articles

32, 33 and 34 of the RGPD.

Article 32 of the RGPD "Security of treatment", establishes that:

"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

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.

3. Adherence to an approved code of conduct under article 40 or to a

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present article.

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 controller or the

manager and has access to personal data can only process said data

following the instructions of the person in charge, unless it is obliged to do so by virtue of the

Law of the Union or of the Member States".

Article 33 of the RGPD, Notification of a breach of the security of the

personal data to the control authority, establishes that:

"1. In case of violation of the security of personal data, the

responsible for the treatment will notify the competent control authority of

accordance with article 55 without undue delay and, if possible, no later than 72

hours after you become aware of it, unless it is unlikely

that said breach of security constitutes a risk to the rights and

freedoms of natural persons. If the notification to the control authority does not have

place within 72 hours, must be accompanied by an indication of the reasons for

the procrastination

2. The person in charge of the treatment will notify the person in charge without undue delay

of the treatment the violations of the security of the personal data of which

be aware.

3. The notification referred to in section 1 must, at a minimum:

a) describe the nature of the data security breach

including, where possible, the categories and number

approximate number of stakeholders affected, and the categories and approximate number

of affected personal data records;

b) communicate the name and contact details of the data protection delegate

data or another point of contact where further information can be obtained;

c) describe the possible consequences of the breach of the security of the

personal information;

d) describe the measures adopted or proposed by the person responsible for the

processing to remedy the data security breach

including, if applicable, the measures taken to mitigate the

possible negative effects.

4. If it is not possible to provide the information simultaneously, and to the extent

where it is not, the information will be provided gradually without undue delay.

5. The data controller will document any violation of the

security of personal data, including the facts related to it, its

effects and corrective measures taken. Such documentation will allow the

control authority verify compliance with the provisions of this article.

And article 34, Communication of a breach of data security

data to the interested party, establishes that:

"1. When the data security breach is likely

entails a high risk for the rights and freedoms of individuals

physical data, the data controller will communicate it to the interested party without delay

improper.

2. The communication to the interested party contemplated in section 1 of this

article will describe in clear and simple language the nature of the violation of the

security of personal data and will contain at least the information and

measures referred to in article 33, section 3, letters b), c) and d).

3. The communication to the interested party referred to in section 1 will not be

required if any of the following conditions are met:

a) the data controller has adopted technical protection measures

and organizational measures and these measures have been applied to the data

affected by the violation of the security of personal data,

in particular those that make personal data unintelligible for

anyone who is not authorized to access them, such as encryption;

b) the data controller has taken further steps to ensure

that there is no longer the probability that the high risk for the

rights and freedoms of the interested party referred to in section 1;

c) involves a disproportionate effort. In this case, you will choose instead

by a public communication or similar measure by which it is reported

equally effectively to stakeholders.

4. When the person in charge has not yet communicated to the interested party the

violation of the security of personal data, the control authority, once

Considering the probability that such a violation involves a high risk, it may require

to do so or may decide that any of the conditions mentioned in

section 3".

The violation of articles 32, 33 and 34 of the RGPD are typified

in article 83.4.a) of the aforementioned RGPD in the following terms:

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

with 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 pursuant to articles 8,

11, 25 to 39, 42 and 43.

(…)"

For its part, the LOPDGDD in its article 71, Violations, states that:

"The acts and behaviors referred to in sections 4,

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

contrary to this organic law.

And in its article 73, for the purposes of prescription, it qualifies as "Infringements

considered serious":

“Based on the provisions of article 83.4 of Regulation (EU) 2016/679

are 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:

(…)

g) The violation, as a consequence of the lack of due diligence,

of the technical and organizational measures that have been implemented in accordance

to what is required by article 32.1 of Regulation (EU) 2016/679”.

r) Failure to comply with the duty to notify the data protection authority

data from a security breach of personal data in accordance

with the provisions of article 33 of Regulation (EU) 2016/679.

s) Failure to comply with the duty to notify the affected party of a violation of

the security of the data in accordance with the provisions of article 34 of the

Regulation (EU) 2016/679 if the data controller had been

required by the data protection authority to carry out such

notification.

The facts revealed in this claim show the

existence of a security incident in the claimed systems allowing the

vulnerability of the same by enabling the system of its electronic headquarters to allow

access to the data related to the register where they appeared in addition to the data

of the components of the claimant's family those of other interested parties.

III

In the present case, the claimant, upon checking in the electronic office of the
claimed, through the secure verification code (CSV), the collective certificate of
registration that his father had requested, the system of the electronic office
returns 23 certificates of various kinds related to the register where they appear
personal data of the components of the family of the claimant and of the interested parties
of the other 22 certificates signed on the same day. All certificates signed on
same day have the same CSV. The claimant requests that since it cannot be
change the CSV after it is generated, an additional field is entered into the system, or
second step where the DNI is requested to be able to discriminate the correct document
before viewing it.

The GDPR defines personal data security breaches as
"all those violations of security that cause the destruction, loss or
accidental or unlawful alteration of personal data transmitted, stored or processed
otherwise, or unauthorized communication or access to such data".

From the documentation in the file, there are clear indications of
that the claimed party has violated article 32 of the RGPD, when there was a breach of
security in their systems allowing access to data related to the
census.

The RGPD in the aforementioned precept does not establish a list of security measures.
security that are applicable in accordance with the data that is the object of
treatment, but establishes that the person in charge and the person in charge of the treatment
apply technical and organizational measures that are appropriate to the risk involved
the treatment, taking into account the state of the art, the application costs, the
nature, scope, context and purposes of the treatment, the risks of probability
and seriousness for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and

proportionate to the detected risk, pointing out that the determination of the measures

technical and organizational information must be carried out taking into account: pseudonymization and

encryption, the ability to ensure the confidentiality, integrity, availability and

resiliency, the ability to restore availability and access to data after a

incident, verification process (not audit), evaluation and assessment of the

effectiveness of the measures.

In any case, when evaluating the adequacy of the level of security,

particularly taking into account the risks presented by the processing of data, such 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 and that could cause damages

physical, material or immaterial.

In this same sense, recital 83 of the RGPD states that:

“(83) In order to maintain security and prevent the treatment from violating the

provided in this Regulation, the person in charge or the person in charge must evaluate

the risks inherent to the treatment and apply measures to mitigate them, such as

encryption. These measures must guarantee an adequate level of security, including

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and the nature of the personal data that must be

protect yourself. When assessing the risk in relation to data security,

take into account the risks arising from the processing of personal data,
such as the accidental or unlawful destruction, loss or alteration of personal data
transmitted, stored or otherwise processed, or the communication or access is not
authorized to said data, susceptible in particular to cause damages
physical, material or immaterial.
In the present case, as evidenced by the facts and within the framework of the
investigation file E/01827/2019 the AEPD on 12/13/2018 notified the
claim to the respondent requesting the provision of information related to the
incident claimed, without receiving any response from this body and,
Despite the previous requirement, it was proven that the data was still being exposed
personal information of the interested parties that were included in the 23 documents of the list that were
obtained by entering the secure verification code of the collective certificate of
registration registration.
It should be noted that the responsibility of the claimed party is determined by
the breach of security brought to light by the claimant, since it is responsible
to make decisions aimed at effectively implementing the measures
appropriate technical and organizational measures to guarantee a level of security adequate to the
risk to ensure the confidentiality of the data and, among them, those aimed at
quickly restore availability and access to data in the event of an incident
physical or technical. However, the documentation provided shows that the
entity not only failed to comply with this obligation, but also had not adopted
no action despite having notified him of the claim informing him of
it.
The RGPD also regulates in its article 33 the notification of violations of
security that may pose a risk to the rights and freedoms of
natural persons to the competent control authority, which in the Spanish case is

of the AEPD.

Therefore, whenever data of a nature is affected in a breach

personnel of natural persons must notify the AEPD and, in addition,

we must notify it within a maximum period of 72 hours from when we have

awareness of the gap.

It should be noted that none of these obligations was met by the

reclaimed; on the contrary, having been informed of the security incident

revealed in the claim, did not send the AEPD any news that

had adopted measures aimed at remedying it, once it had

knowledge of it.

As there is no evidence that, in accordance with what is stated in the

article 34, which would have communicated to the interested parties the violation of the security of

personal data without undue delay once it became aware of it.

However, it is also true that by opening the agreement to start the

sanctioning procedure, in writing of allegations dated 03/06/2020 on

claimed confirmed the infraction committed and stated that it was true that in the

issuance of the certificate indicated by the claimant, other

certificates made that day and that were digitized together.

It has also indicated that in relation to the incidence produced by the Technician

Informático had issued a report on the causes that motivated the same and that

originated the claim as well as the measures adopted to prevent it from being

similar events occur in the future. In addition, the Head of the Service Bureau

of Citizen Attention where said certificates are issued also issued

report from which it can be deduced that these certificates are currently of the class

they are issued individually and automatically.

In accordance with the foregoing, it is estimated that the respondent is

responsible for breaches of the GDPR: articles 32, 33 and 34, breaches

all of them typified in its article 83.4.a).

However, also the LOPDGDD in its article 77, Regime applicable to

certain categories of controllers or processors, establishes the

Next:

IV

"1. The regime established in this article will be applicable to treatments

of which they are responsible or entrusted:

a) The constitutional bodies or those with constitutional relevance and the

institutions of the autonomous communities analogous to them.

b) The jurisdictional bodies.

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

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

d) Public bodies and public law entities linked or

dependent on the Public Administrations.

e) The independent administrative authorities.

f) The Bank of Spain.

g) Public law corporations when the purposes of the treatment

related to the exercise of powers of public law.

h) Public sector foundations.

i) Public Universities.

j) The consortiums.

k) The parliamentary groups of the Cortes Generales and the Assemblies

Autonomous Legislative, as well as the political groups of the Corporations

Local.

2. When the managers or managers listed in section 1

committed any of the offenses referred to in articles 72 to 74 of

this organic law, 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 on which it reports hierarchically, where appropriate, and those affected who have

the condition of interested party, if any.

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

data protection will also propose the initiation of disciplinary actions

when there is sufficient evidence to do so. In this case, the procedure and

sanctions to apply will be those established in the legislation on disciplinary regime

or sanction that results from application.

Likewise, when the infractions are attributable to authorities and managers,

and the existence of technical reports or recommendations for treatment is proven

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 informed of the resolutions that fall in relation to the measures and actions referred to the previous sections.

5. They will be communicated to the Ombudsman or, where appropriate, to the institutions analogous of the autonomous communities the actions carried out and the resolutions issued under this article.

6. When the competent authority is the Spanish Agency for the Protection of Data, it will publish on its website with due separation the resolutions referred 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 would have committed the infringement.

When the competence corresponds to a regional protection authority of data will be, in terms of the publicity of these resolutions, to what is available its specific regulations.

According to the available evidence, said conduct constitutes by the claimed the infringement of the provisions of articles 32.1, 33 and 34 of the RGPD.

It should be noted that the RGPD, without prejudice to the provisions of article 83, contemplates in its article 77 the possibility of resorting to the sanction of warning to correct the processing of personal data that is not in accordance with your forecasts, when those responsible or in charge listed in section 1 committed any of the offenses referred to in articles 72 to 74 of this organic law.

In the present case, taking into account the nature of the infraction and having

account that the respondent in writing dated 03/06/2020 has informed this Agency

the circumstances in which the incident that led to the claim occurred, as well as

as well as the measures adopted in order to prevent events such as the one claimed from happening again.

occur in the future. Likewise, it recognizes the error made and that in the issuance of the

certificate indicated by the claimant other certificates made were included

that day being digitized together and sent to the digital circuit so that the

file content contained the same signature and same CSV; in the face of this incident

Municipal Computer Technician has issued a report on the causes that motivated the

incidence and the technical measures adopted to prevent events from occurring

similar in the future. In the same way, the Bureau Chief of the Service of

Citizen Service where these certificates are issued has issued a report

pointing out that the individual, collective and historical individual certificates and

groups that are issued from the Register of Inhabitants is done in a

individualized and automated.

Therefore, it is considered that the respondent's response was reasonable and

diligently, acknowledging the facts and immediately correcting the errors

committed, not having evidence of other claims by the

persons affected and adopting adequate measures to avoid any anomaly or

future incident that may occur.

However, warn the respondent that in the event that any

other security incident that may pose a risk to the rights and

freedoms of natural persons their obligation to notify the supervisory authority

as well as those potentially affected by the incident without undue delay once

had knowledge of it.

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

graduation of sanctions whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE BAENA CITY COUNCIL, with NIF P1400700I, for a

infringement of articles 32.1, 33 and 34 of the RGPD, typified in article 83.4 of the

RGPD, a penalty of warning in accordance with article 77.2 of the

LOPDGDD.

SECOND: NOTIFY this resolution to the BAENA CITY COUNCIL, with

NIF P1400700I.

THIRD

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

: COMMUNICATE this resolution to the Ombudsman,

In accordance with the provisions of article 50 of the LOPDGDD, the

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

month 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, the firm resolution may be provisionally suspended in administrative proceedings

if the interested party expresses his intention to file a contentious appeal-

administrative. If this is the case, the interested party must formally communicate this

made by writing to the Spanish Agency for Data Protection,

introducing him to

the agency

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

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

must 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

precautionary suspension.

Electronic Registration of

through the

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es