Procedure No.: PS/00416/2020

 RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claimant) on 01/13/2020 filed

claim before the Spanish Data Protection Agency. The claim is

directed against the CITY COUNCIL OF ALBUIXECH with NIF P4601400G (hereinafter,

the claimed). The reasons on which the claim is based are in summary:

that through the website of the claimed party you can access personal data of

neighbors such as DNI, telephone, disability, economic situation; providing several of

web page links that display documents with personal data.

SECOND: In accordance with the provisions of article 65.4 of the LOPDGDD, the

Transfer of your claim to the respondent so that he proceeded to analyze it and give

response within one month on the incident claimed. On date 06/03/2020,

the respondent, responded to the previous request.

THIRD: On 06/09/2020, after analyzing the documentation that was in the

file, a resolution was issued by the director of the AEPD, agreeing not to admit

to process the claim. The resolution was notified to the appellant on the date

06/09/2020.

FOURTH: On 06/09/2020, the claimant filed an optional appeal for

replacement against the resolution issued in file E/02285/2020, showing its

disagreement with the contested resolution, invoking similar arguments that the

contained in his initial claim and stating that the City Council had not

taken the corresponding measures because as of 06/09/2020, it was still being accessed

to the documents already mentioned in the claim and together with the appeal,

new relevant documentation for the purposes of the above.

FIFTH: On 11/06/2020, after the checks carried out by accessing

any of the links that lead to pages with information containing data

personal data, it is found that several of the published documents containing

information with personal data have not been deleted or anonymised,

resolving the reversal appeal filed against the resolution of this Agency

issued on 06/09/2020, and agree on the admission of the claim presented.

SIXTH: On 01/25/2021 the Director of the AEPD agreed to initiate a procedure

sanctioning the person claimed for the presumed infractions of articles 5.1.f) and 32.1

of the RGPD, typified in articles 83.5.a) and 83.4.a) of the aforementioned Regulation.

SEVENTH: Once the initiation agreement was notified, on 02/12/2021 the respondent requested a copy of the

file and extension of the term that was sent and granted, respectively,

by the procedure instructor.

On 02/18/2021, the respondent submitted a written statement of allegations stating. in

synthesis: that although initially a plugin was installed to block access to the

contents of the web page of the claimed, the IT department that I deal with

to solve the incident in the first instance was aware that the measure was

seemed insufficient because although the content could not be accessed, it continued to be

possible to access by knowing the URL of the published files; that for this reason

carried out a migration of the web to another server so that all the content to the

that could have been accessed is completely eliminated and not being possible

have access from the time the migration was performed.

EIGHTH: On 02/24/2021 a period of practice tests began,

remembering the following

- Consider reproduced for evidentiary purposes the claim filed by the

claimant and his documentation, the documents obtained and generated by the

Inspection Services that are part of file E/09211/2020.

- Consider reproduced for evidentiary purposes, the allegations to the agreement of

home filed by the respondent

NINTH: On 04/05/2021, a Resolution Proposal was issued in the sense that

sanction the claimant for infringement of articles 5.1.f) and 32.1 of the RGPD,

typified in articles 83.5.a) and 83.4.a) of the RGPD, with warning of

in accordance with article 77 of the LOPDGDD.

After the legally stipulated period, the respondent had not submitted a written

of allegations.

TENTH: Of the actions carried out in this proceeding, they have been

accredited the following:

PROVEN FACTS

FIRST: 01/13/2020 has entry in the Spanish Agency for Data Protection

written by the claimant, stating that through the web page of the claimed

can access personal data of neighbors such as ID, telephone, disability,

economic situation; providing several of the web page links that they show

documents with personal data.

SECOND: On 06/09/2020, a resolution was issued agreeing to the non-admission of

the claim.

THIRD: On 06/09/2020 the claimant filed an optional appeal for reconsideration

showing their disagreement with the resolution issued, stating that the claimed

had not taken the measures since the data could still be accessed

personal data contained in the information published on the web, providing new

relevant documentation for the purposes of the above, issuing an approving resolution

on 11/06/2020.

FOURTH: The respondent has stated that: "Before receiving the start of the

sanctioning procedure, specifically on 12/01/2020, a

migration of the web www.albuixech.es to another server, so all the content …

is already completely deleted and it is not possible to have access from the moment

that the migration took place

It also states that “The following measures have been adopted on the new website

to prevent this incident from happening again:

(...).

FIFTH: The respondent has provided a screenshot of the web page where

it is not possible to access any content and where the information containing

the personal data that gave rise to the claim and that is currently being

found eliminated.

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

II

The facts denounced are specified that through the website

http//www.albuixech.es/wp-content/uploads/ ownership of the claimed could be accessed

to personal data of neighbors such as DNI, telephone, disability, economic situation

and that despite the fact that he had stated that he had resolved the incident, no action had been taken.

taken the corresponding measures since it was possible to continue accessing the data

of the neighbors.

In the first place, said treatment could constitute an infringement of the

Article 5, Principles related to the treatment, of the RGPD that establishes 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 processing or

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

of appropriate technical or organizational measures ("integrity and

confidentiality").

(…)"

Article 5, Duty of confidentiality, of the new Organic Law 3/2018, of 5

December, Protection of Personal Data and guarantee of digital rights

(hereinafter LOPDGDD), states that:

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

people who intervene in any phase of this will be subject to the duty of

confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary

of the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will remain

even when the relationship of the obligor with the person in charge or person in charge had ended

of the treatment".

Second, article 32 of the RGPD "Security of treatment",

III

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".

IV

Article 83.5 a) of the RGPD, considers that the infringement of "the principles basic for the treatment, including the conditions for the consent in accordance with of articles 5, 6, 7 and 9" is punishable, in accordance with section 5 of the mentioned article 83 of the aforementioned GDPR, "with administrative fines of €20,000,000 maximum or, in the case of a company, an amount equivalent to 4% as maximum of the overall annual total turnover of the previous financial year,

opting for the highest amount.

On the other hand, the LOPDGDD, for prescription purposes, in its article 72 indicates:

“Infringements considered very serious:

1. Based on the provisions of article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

suppose a substantial violation of the articles mentioned in that and, in

particularly the following:

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

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

(…)”

The violation of article 32 of the RGPD is typified in the article

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

v

"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".

(…)"

SAW

The proven facts evidence access through the website

http//www.albuixech.es/wp-content/uploads owned by the claimant to the data of

personal character of local residents (ID, telephone number, disability, situation

economy, etc.), despite having told this AEPD that he had given

solution to the incident, breaking and violating the measures of a technical nature and

organization and the duty of data confidentiality.

As stated in the records and accredited in the proven facts of the

procedure has been accredited that the filing resolution of the

initial claim, the claimant filed an optional appeal for reconsideration against the

relapsed resolution showing their disagreement and stating that the claimed party does not

had taken the appropriate measures since, despite what was alleged, the

accessing the data on the municipal website, contributing together with the written appeal

new relevant documentation.

After the analysis and checks carried out, it was found that there was

published documents containing information with personal data that

had not been eliminated or anonymized, estimating the appeal and agreeing to the

acceptance of the claim filed.

Therefore, the entity's actions constitute a violation of the principles of

confidentiality and data security, regulated in articles 5.1.f) and 32.1

of the RGPD, and typified in articles 83.5.a) and 83.4.a) of the RGPD.

However, in order to clarify the terms of the incidence produced

and that led to the opening of this sanctioning procedure, the defendant

By means of a letter dated 02/18/2021, it indicated that although initially a

WP Content Copy Protection Pro plugin to block access to documents

existing on the website of the City Council and carry out the elimination of the

files containing personal data published on the aforementioned page, after

the receipt of the agreement to open the procedure the IT service treated

at first to solve the incident reaching the conclusion that the

measure adopted (install a plugin to block access to the web), it seemed

insufficient since although it prevented access to the contents, it continued to be

possible to access them if the URL of the files was known

published.

For this reason, the migration of the entity's website to another server was carried out

that I determine that the content that could have been previously accessed

as of that date, it was eliminated and it was not possible to access it from the

when the migration was performed.

In order to avoid incidents such as the one that occurred, on the new website

a series of technical measures were adopted: remove access to the wp-folder

content and its content through .htaccess; check before serving permissions

WP using the is-luger-logged-in function, to retrieve a file for a

subfolder of wp-content, etc.

In addition, the respondent has indicated that he assumes his responsibility as

consequence of the infractions committed, although he considers that they should be taken into

account the efforts made to improve security measures in order to

to guarantee the security and confidentiality of the personal data of

which is responsible and that the violation is not due to inaction or lack of

proactivity in complying with data protection regulations.

On the other hand, it should be noted that the respondent provides screen printing

of the web page where the content of the personal data should be

that caused the claim and that are currently eliminated, not

being possible to have access to them.

The LOPDGDD in its article 77, Regime applicable to certain categories

responsible or in charge of the treatment, establishes the following:

7th

"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.

In the case at hand, in accordance with the evidence from which

available and without prejudice to what results from the investigation, said conduct could

constitute, on the part of the claimed, the possible infringement of the provisions of article

5.1.f) and 32.1 of the GDPR.

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.

Likewise, it is contemplated that the resolution issued will establish the measures

that it is appropriate to adopt so that the conduct ceases, the effects of the infraction are corrected

that had been committed and its adaptation to the requirements contemplated in the

articles 5.1.f) and 32.1 of the RGPD, as well as the provision of supporting means of the

compliance with what is required.

However, it is considered that the answer formulated by the respondent in

letter dated 02/18/2021 has been reasonable, correcting the incident produced not

proceeding to urge the adoption of additional measures to those already taken by the

claimed, which is one of the main purposes of the proceedings regarding

of those entities listed in article 77 of the LOPDGDD, having

the suspension of the website of the entity where the

information containing the personal data of the neighbors having

migrated it to another server and taking a series of measures to prevent it from being

occur events such as those that gave rise to the claim.

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 ALBUIXECH CITY COUNCIL, with NIF P4601400G, by

an infringement of article 5.1.f) of the RGPD, typified in article 83.5.a) of the RGPD,

a sanction of warning, in accordance with article 77 of the LOPDGDD.

SECOND: IMPOSE ALBUIXECH CITY COUNCIL, with NIF P4601400G, by

an infringement of article 32.1 of the RGPD, typified in article 83.4.a) of the RGPD,

a sanction of warning, in accordance with article 77 of the LOPDGDD.

THIRD

with NIF P4601400G.

: NOTIFY this resolution to the ALBUIXECH CITY COUNCIL,

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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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