 File No.: PS/00361/2021

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 complaining party), on February 17,

2021, filed a claim with the Spanish Data Protection Agency. The

claim is directed against the CITY COUNCIL OF ALBACETE with NIF P0200300B

(hereinafter, the claimed party). The grounds on which the claim is based are

following:

Specifically, you state that, by accessing your private area to check the status in

who was processing your file, has viewed personal data

of other people (names, DNI/NIE, addresses and telephone numbers) and registration requests

of other administrators.

Together with the claim, it provides documents from the electronic office regarding

to other requests for deregistration in the Municipal Register of Inhabitants, with

visible data of entry registration number, name and surname of the person

procedure applicant.

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

Public (hereinafter, LPACAP), was collected on March 22, 2021, as

It is stated in the acknowledgment of receipt that is in the file.

On April 21, 2021, this Agency received a written response

indicating that when the claimant accesses electronically, (through the use of their

recognized digital certificate), on 02-17-2021 to the electronic file processed

to the effect related to communications/requests for deregistration in the Register

Municipality of Inhabitants corresponding to the month of August 2020, existed within

of the same, five folders of documents of other requests, with the only data

visible entry registration number and the name and surname of the person

applicant in the proceedings, (i.e. the person in question could not be identified)

question, due to the dissociation that exists, as it does not appear together with his name and surnames

your ID number or passport), which since they are requests for the same

nature are accumulated in files that are created for this purpose on a regular basis

monthly, all in accordance with the legal precepts of Law 39/2015, of 1

of October, of the Common Administrative Procedure of the Public Administrations

(article 58) and adds that there must be a subsequent action (conscious and deliberate)

by the person accessing the file, to click voluntarily

in the tab to open each of the folders of other citizens who have

presented an instance with the same purpose as yours, to view the data

personal and identifying, since all those that have included that

interested in your application: DNI/NIE/Passport, postal address and

registration and contact telephone numbers. Lastly, he adds that they have been carrying out

this processing of registration/registration files in the Municipal Register of Inhabitants

of this municipality in this way, since September 19, 2016, the date on which

The electronic processing begins, without to date they have received any

claim these features.

THIRD: On July 2, 2021, in accordance with article 65 of the

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

FOURTH: On February 18, 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.f) 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 February 22, 2022, as stated in the certificate that

work on file.

Once notified of the aforementioned initiation agreement, the respondent filed a written

allegations in which, in summary, it stated that, given the need on the part of the

Albacete City Council, to adhere to the technological model developed and

implemented by the Provincial Council for the provision of services of

Electronic Administration, the Provincial Council assumed the task of managing the

electronic administration services of the City Council and technical collaboration in

matter of definition of types of files, exchange formats and

interoperability, it also stated that the tool for the Management System of

Electronic Files (SEGEX) is owned by the Provincial Council of Albacete and put to

disposition of the different City Councils to facilitate the management of files, for which the responsibility would fall on the Diputación itself, which in view of the citizen's claim, the City Council sent a letter to the Provincial Council requesting the modification in the configuration of the established access levels by default by the tool itself and that they have adopted security measures opportune to mitigate the existing risk of access to personal data of the interested parties linked to the same file, for which it requests the file of the performances.

FIFTH: On April 12, 2022, a resolution proposal was formulated, proposing:

<< That by the Director of the Spanish Agency for Data Protection, the CITY COUNCIL OF ALBACETE, with NIF P0200300B, for an infringement of article 5.1. f) of the RGPD, in accordance with the provisions of article 83.5 of the RGPD, qualified as very serious for prescription purposes in article 72.1 a) of the LOPDGDD and infringement of article 32 of the RGPD, in accordance with the provisions of article 83.4 of the cited RGPD, qualified as serious for prescription purposes in article 73 section f) of the LOPDGDD, a sanction of warning. >>

The aforementioned motion for a resolution was sent, in accordance with the rules established in Law 39/2015, of October 1, on the Common Administrative Procedure of the Public Administrations (hereinafter, LPACAP), by electronic notification, being received on April 13, 2022, as stated in the certificate that works

on the record.

SIXTH: On April 28, 2022, the respondent filed a written statement

allegations to the Resolution Proposal, in which, in summary, the

arguments already exposed in the previous arguments.

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 February 17, 2021, the complaining party filed

claim before the Spanish Agency for Data Protection, due to a violation

security of personal data.

SECOND: It is verified that the claimant has been able to access documents

from the electronic office of the City Council of Albacete relating to other

requests for deregistration in the Municipal Register of Inhabitants, with data

visible entry registration number, name and surname of the requesting person

of the procedure.

THIRD: The respondent states that, from the management unit of the registry of

inhabitants, to speed up the procedure, a single SEGEX file is made in the

that the requests that are made during a month of all the

interested in unsubscribing from the Register. The main cause of this violation of

security is due to the fact that each document that is created in said file comes

configured by default so that all the current interested parties of the file and the

that are added later, can access said document. The cause

Secondary security violation is because this default setting

is not changed manually by the file manager, to indicate that

Only the interested party is the one who accesses the document.

Likewise, it states that it has proceeded to implement the corrective measures

adequate to avoid the repetition of similar events in the future.

The

documentation provided is incorporated into the file.

FOUNDATIONS OF LAW

Yo

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

In accordance with the powers that article 58.2 of 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.”

II

In relation to the statements made by the claimed party, reiterating

basically on the arguments already presented throughout the procedure

sanctioning, it should be noted that all of them were not only analyzed and

rejected, but were taken into account to formulate the Proposal for

resolution, whose Legal Grounds remain fully in force, and that is

summary in the following:

“In the present case, the entity claimed is responsible for data processing.

data, since, in accordance with article 11 of Law 40/2015, of October 1, of

Legal Regime of the Public Sector:

"1. Carrying out activities of a material or technical nature of the competition

administrative bodies or Public Law Entities may be found

recommended to other bodies or Entities of Public Law of the same or different

Administration, provided that these activities are among its powers, for reasons

effectiveness or when they do not have the appropriate technical means for their performance.

No.

The management encomiendas may not have as their object benefits of

contracts regulated in the public sector contract legislation. In that case,

its nature and legal regime will be adjusted to the provisions of this.

2. The management entrustment does not imply transfer of ownership of the competition

nor of the substantive elements of its exercise, being the responsibility of the organ or

Entrusting entity dictate how many acts or resolutions of a legal nature give

support or in which the specific material activity object of entrustment is integrated.

In any case, the entrusted Entity or body will have the status of manager

of the processing of personal data to which you may have access in

execution of the management entrustment, being applicable the provisions of the

protection of personal data.”

Article 4.7 of Regulation (EU) 2016/679, of the European Parliament and of the Council,
of April 27, 2016, regarding the protection of natural persons in what
regarding the processing of personal data and the free circulation of these data by
which repeals Directive 95/46/EC (General Data Protection Regulation -
RGPD-) defines the person in charge of the treatment or responsible as "the natural person or
legal entity, public authority, service or other body which, alone or jointly with others,
determine the purposes and means of the treatment; if the law of the Union or of the
Member States determines the purposes and means of processing, the data controller
treatment or the specific criteria for their appointment may be established by the
Law of the Union or of the Member States."

Likewise, the aforementioned Regulation refers -in section 8 of its article 4- to the
in charge of the treatment or in charge as "the natural or legal person, authority
public, service or other body that processes personal data on behalf of the
data controller".

In this sense, it should be remembered that the figure of the person in charge of the treatment obeys the
the need to respond to phenomena such as the outsourcing of services by
part of the companies and other entities, so that in those cases in which
the data controller entrusts a third party with the provision of a service
that requires access to personal data by it, said access and
treatment is carried out by the person in charge, in the name and on behalf of the person in charge,
as if he were the one who carried it out.

Report 0064/2020 of the Legal Office of the AEPD has emphatically expressed
that the RGPD has meant a paradigm shift when dealing with the regulation of the right
right to the protection of personal data, which is based on the principle of
"accountability" or "proactive responsibility" as has been repeatedly pointed out

the AEPD (Report 17/2019, among many others) and is included in the Statement of Motives

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

and guarantee of digital rights (LOPDGDD)": "the greatest novelty presented by the

Regulation (EU) 2016/679 is the evolution of a model based, fundamentally, on

in the control of compliance to another that rests on the principle of responsibility

active, which requires a prior assessment by the person in charge or by the person in charge of the

treatment of the risk that could be generated by the treatment of personal data.

personnel to, based on said assessment, adopt the appropriate measures".

Article 5.2 of the RGPD establishes that "the controller will be

responsible for compliance with the provisions of paragraph 1 and able to demonstrate it

("proactive responsibility")". This means that the person in charge must guarantee the

effective application of the principles of treatment both at the time of determining

the means of treatment and during the treatment itself, through the

articulation of a series of measures, which must be subject to review and

regular update. This implies that the aforementioned person in charge is the one who assumes

own responsibility directing and coordinating the matter, including that of the staff

that provides services to you.

For these purposes, what is stated in the following recital of the

GDPR:

74. "The responsibility of the data controller for data processing must be established.

any processing of personal data carried out by himself or on his behalf. In

In particular, the person responsible must be obliged to apply timely and effective measures
and must be able to demonstrate compliance of the processing activities with the
this Regulation, including the effectiveness of the measures. These measures must have
taking into account the nature, scope, context and purposes of the treatment, as well as the
risk to the rights and freedoms of natural persons."

On the infringement of lack of security measures for data processing, the
The National High Court stated in various sentences: (June 13, 2002 -appeal no.
1,517/2001 -, February 7, 2003 -appeal no. 1,182/2001 -, January 25, 2006 -
appeal no. 227/2004 -, March 28, 2006 resource 478/2004, June 28, 2006 -
resource no. 290/2004 -, March 24, 2015 -appeal no. 269/2013 - and June 25
2015 -resource no. 90/2014), that the obligation arising from the implementation of
security measures regarding personal data, "there is no
complies with the adoption of any measure, since they must be those necessary to
guarantee those objectives that the precept marks, and of course, it is not enough with the
formal approval of the security measures, since it is required that those
are established and implemented effectively. (…)"

Faced with the risk that a citizen who accesses his file may open each
one of the folders of other citizens who have presented an instance with the same
same purpose as yours, being able to view personal and identifying data, is obtained
lack of these measures. The City Council made the decision to accumulate several
records of deregistration in the Municipal Register, in application of article 57 of the Law
39/15 (the City Council erroneously mentions article 58). This decision is yours
of the City Council and does not obey the design of the tool, which facilitated the internal access
because of information from other stakeholders, when it really doesn't make accrued sense.
formulate files that, even referring to the same matter, are from different interested parties.
cough. The computer tool allowed City Council staff to select which

type of interested parties could have access to the file. Although by default the option is

“all concerned”, the selection could be changed manually (which it should have done).

cer the City Hall staff in this case). It was not done, which, again, led

that “all interested parties” had access. And, as has been pointed out, “all the interests

sados” were those of all the files that, without any sense, had been accumulated

sides.

These preventive measures, aimed at guaranteeing the confidentiality, integrity and

availability of the data, which must be established, must also be subject to

follow-up on its compliance and effectiveness, as well as when the

circumstances of the treatment, attending and contemplating in its case, any

incident that may occur.

Therefore, the data controller must carry out an analysis of the

risks of data processing, implementing technical and organizational measures

appropriate to apply the principles of data protection and integrate the guarantees

necessary in the treatment, in order to meet the requirements of the RGPD, and must be able to

demonstrate that the treatment is in accordance with the provisions of the aforementioned standard.

Finally, among the measures adopted after the breach, the City Council states

which sent a letter to the Provincial Council requesting the modification in the

configuration of the access levels established by default by the

tool. In this sense, a minimum diligence of the City Council would have to

have had them request it earlier. And, in any case, he should have watched, case by case, that

each file was accessed only by those interested in it. Being, thus

things, and even when in the present case the defendant entity had proceeded, in

the moment of determining the means, to design and implement measures

chords, this would not exempt him from continuing to be responsible for the effectiveness of said

measures during the whole time in which the collection and treatment had taken place

of personal data.

In the present case, it is accredited that the personal data of users of the

Electronic Records Management System tool were improperly

exposed to third parties from the information system itself, violating the principles

of integrity and confidentiality, both established in article 5.1.f) of the RGPD.

Therefore, non-compliance with data protection regulations must be fully

mente imputed to the data controller, by not acting actively and effectively

in stipulating and enforcing the appropriate specifications to properly carry out

properly in time, the treatment entrusted on your behalf.

Accordingly, the claims must be dismissed."

III

Article 5.1f)

Article 5.1.f) of the RGPD establishes the following:

"Article 5 Principles relating to the treatment

1. The personal data will be:

(…)

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

including protection against unauthorized or unlawful processing and against

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

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

In the present case, it is proven that personal data of citizens working

in the computer application for the management of the municipal register of inhabitants were

unduly exposed to third parties, violating the principles of integrity and

confidentiality, both established in the aforementioned article 5.1.f) of the RGPD.

Classification of the infringement of article 5.1f) of the RGPD

IV

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)

the basic principles for the treatment, including the conditions for the

consent under articles 5, 6, 7 and 9;”

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

following: "The acts and behaviors 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.

v

Article 32 of the GDPR

Article 4.12 of the RGPD establishes that it is considered "violation of the security of the

personal data: any breach of security that results in the destruction, loss

or accidental or unlawful alteration of personal data transmitted, stored or

otherwise processed, or unauthorized communication or access to said data."

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).

Recital 75 of the RGPD lists a series of factors or assumptions associated with

risks for the guarantees of the rights and freedoms of the interested parties:

“The risks to the rights and freedoms of natural persons, serious and

variable probability, may be due to the processing of data that could cause

physical, material or non-material damages, particularly in cases where

that the treatment may give rise to problems of discrimination, usurpation of

identity or fraud, financial loss, reputational damage, loss of

confidentiality of data subject to professional secrecy, unauthorized reversal of the

pseudonymization or any other significant economic or social damage; in the

cases in which the interested parties are deprived of their rights and freedoms or are

prevent exercising control over your personal data; In cases where the data

treated personalities reveal ethnic or racial origin, political opinions, religion

or philosophical beliefs, militancy in trade unions and the processing of genetic data,

data relating to health or data on sex life, or convictions and offenses

criminal or related security measures; In cases where they are evaluated

personal aspects, in particular the analysis or prediction of aspects related to the
performance at work, economic situation, health, preferences or interests
personal, reliability or behavior, situation or movements, in order to create or
use personal profiles; in the cases in which personal data of
vulnerable people, in particular children; or in cases where the treatment
involves a large amount of personal data and affects a large number of
interested."

In the present case, the lack of implementation of technical and organizational measures has
caused access by unauthorized third parties to the data stored in the system of
information from the electronic headquarters of the claimed party, thereby violating the
article 32 of the RGPD.

In this regard, and as has been stated in the previous foundation, the City Council
The administration made the decision to accumulate various records of removal from the Municipal Register.
cipal, in application of article 57 of Law 39/15 (erroneously the City Council
mentions article 58). This decision belongs to the City Council and does not obey the di-
design of the tool, which facilitated improper access to the information of other inte-
resents, when it really does not make sense to accumulate files that, even referring-
It is the same matter, they are from different stakeholders. The computer tool allows
It was up to City Hall staff to select what type of interested parties could have actions.
cess to the file. Although by default the option is "all interested", the selection
tion could be changed manually (which City Hall staff had to do
in this case). It was not done, which, again, led to "all those interested" having

great access. And, as has been pointed out, "all stakeholders" were those of all ex-

requests that, without any sense, had been accumulated.

Finally, and as also stated in the previous rationale, among the measures

adopted after the breach, the City Council states that it sent a letter to the

Provincial Council requesting the modification in the configuration of the levels of

access established by default by the tool itself. In this sense, a

minimum diligence of the City Council should have made them request it before.

And, in any case, he had to monitor, case by case, that each file was accessed only

by those interested in it. Being, thus the things, and even when in the case

present, the respondent entity would have proceeded, at the time of determination of

the media, to design and implement appropriate measures, this would not exempt him from

remain responsible for the effectiveness of such measures for as long as

in which the collection and processing of personal data had taken place.

In the present case, it is accredited that the personal data of users of the

Electronic Records Management System tool were improperly

exposed to third parties from the information system itself,

The consequence of this lack of mandatory security measures was

the exposure to third parties of the personal data of citizen users of the

electronic office. In other words, those affected have been deprived of control over

your personal information.

In this case, the Internet search, for example, of the name, surnames, ID or email

email of some of those affected can offer results that combining them

with those now accessed by third parties, allow us access to other applications of

those affected or the creation of personality profiles, which need not have

been consented by its owner.

This possibility represents an added risk that must be assessed in the study of

risk management and that increases the demand for the degree of protection in relation to

the security and safeguarding of the integrity and confidentiality of these data.

This risk must be taken into account by the data controller, who must

establish the necessary technical and organizational measures to prevent the loss of

control of the data by the data controller and, therefore, by the data controllers.

holders of the data that provided them.

Classification of the infringement of article 32 of the RGPD

SAW

Article 83.4 of the RGPD provides 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.

7th

Responsibility

Establishes Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in

Chapter III on the "Principles of the power to impose penalties", in 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

with the consequence of breaching the principle of confidentiality constitutes the

element of guilt.

viii

Sanction

Article 83.7 of the RGPD adds:

“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 f) of the RGPD, typified in article

83.5 of the RGPD, and for violation of article 32 of the RGPD, typified in article 83.4 of the GDPR.

IX

Measures

Article 58.2 of the RGPD provides: "Each control authority will have 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.f) 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 the CITY COUNCIL OF ALBACETE with a WARNING, with NIF P0200300B, for an infringement of article 5.1.f) of the RGPD, typified in the article 83.5 of the RGPD.

SECOND:

SANCTION with a WARNING to the CITY COUNCIL OF ALBACETE, with NIF P0200300B, for an infringement of article 32 of the RGPD, typified in article 83.4 of the RGPD.

THIRD: REQUEST the ALBACETE CITY COUNCIL 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 ALBACETE CITY COUNCIL.

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

938-050522

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es