 File No.: PS/00134/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: On August 15, 2020, A.A.A. (hereinafter, the claimant)

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

STATE AGENCY SUPERIOR COUNCIL OF SCIENTIFIC RESEARCH

with NIF Q2818002D (hereinafter, the claimed).

The claimant submitted a request for public information addressed to the respondent, for

through the Government Transparency Portal. On June 13, 2019, the

defendant issued a resolution on his case allowing partial access to the

requested information, openly publishing the resolution, since, although

placed a black rectangle above his name and surnames, this text was not

deleted, and it appeared in the pdf, so it was possible to access and locate it

using an internet browser or pdf editor. The resolution is in the URL:

***URL.1. In addition, the published resolution includes the CSV code, allowing

view the original document containing the personal data of the

claimant.

Date on which the claimed events took place: February 1, 2021.

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

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), said claim was transferred to the respondent, so that

proceed to 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.

On December 17, 2020, a response was received from the respondent, indicating that:

"However, considering the time that has elapsed and the request of the affected party, proceeds to consider your request and respond to it by adopting the measures necessary".

THIRD: On January 29, 2021, in accordance with article 65 of the LOPDGDD, the Director of the Spanish Data Protection Agency agreed admit for processing the claim filed by the claimant against the respondent.

FOURTH: In view of the facts denounced in the claim and the documents provided by the claimant, of the facts and documents of which she has had knowledge of this Agency, the Subdirectorate General for Data Inspection 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), having knowledge of the following ends:

INVESTIGATED ENTITY

STATE AGENCY SUPERIOR COUNCIL OF SCIENTIFIC RESEARCH,

with NIF Q2818002D and with address at c/ Serrano 117, 28006, Madrid (Madrid).

RESULT OF THE INVESTIGATION ACTIONS

On 02/01/2021 the following checks are carried out:

- You get a screenshot of the URL:

***URL.1. It is verified that it is a pdf document in which, performing a

search for the text “A.A.A.”, an occurrence is found (one of one: 1/1), although

said text is not displayed as it appears to be hidden with a black rectangle. I know

Verify that you can extract from this document, by copying and pasting, the text of

below the black rectangle, resulting: “Dª A.A.A.”.

- It is verified that the Google search engine finds the text “A.A.A.” in the referred

pdf document.

On 02/10/2021 the following checks are carried out:

- URL access is attempted:

***URL.1 Checks the page is no longer found.

- It is verified that using the Google search engine the text "A.A.A." it follows

finding. When accessing through the link shown by Google, the

page post. It is verified that the cited page is in the cache of

Google.

On 02/10/2021, information and documentation has been requested from the claimant with

the following results:

About the reasons why the name and surnames of the

claimant on the website www.csic.es and the date on which the publication was removed,

The representatives of the entity make the following statements in this regard:

“The reasons have already been answered in writing by the delegate for the Protection of

Data from 10-20-2020, which is attached and reproduced:

Under Law 19/2013, of December 9, on transparency, access to

public information and good governance (LT) information is provided to the

society in general being applicable, yes, the principles of minimization

of data and the criteria of damage, weighting, proportionality.

Criteria applicable to both active advertising - compulsory, periodic and updated

(art 5 LT)- as well as that disclosed as a result of the exercise by the applicant

of the right of access (Chap. III LT).

Double track that will end in a convergence in disclosure because the

right of access is an additional way to make information public

that is not initially included in active advertising, which is incorporated into the

have to include the information of legal relevance provided for in article 7

of the LT, among which will be found the answers given to the requests for

access.

However, this transfer of information between that provided in response to

requested access and active advertising requires prior dissociation unless

relevant circumstances concur (art 14. 3 LT).

In this sense, two circumstances must be taken into account:

1) On the one hand, the political relevance of the applicant that can justify and on the

any case must be taken into account regarding the disclosure of your identity

which derives from the fact that, in any case, its possible disclosure is not

disproportionate

(…)

And in this sense they are still freely accessible to the public today.

information in this regard by the will of the affected party, resulting

applicable provisions of the article of the 15 LT: «1. If the requested information

contained personal data that reveal the ideology, union affiliation, religion

or beliefs, access may only be authorized in the event that

have the express written consent of the affected party, unless

said affected party would have manifestly made public the data with

prior to requesting access

(…)

What unfolds next.

1) Public figures have a more limited sphere of privacy

politician are subject to greater exposure of their data to public opinion

public, voluntarily diluting the privacy of their data and their actions.

Circumstance that has been ratified by various sources:

-The Article 29 Working Group

It has issued an interpretive guide on the concepts developed by the

CJEU in relation to the right to be forgotten, which are transcendent for the

present course. In it, he understands that this right is limited in the

people with public relevance and who are "public figures" who are

destined to develop a role in public life and/or use resources

public for the development of the activity.

The Supreme Court

Which exposes in (for all) Judgment 1175/2020 of 17 Sep. 2020, the

factors to weigh public relevance and data protection.

Specify the content of the weighting factors related to relevance

public information, from its objective (activity) and subjective perspective

(public or private nature of the affected person); as well as the incidence of

time factor in the quality of the data of the interested party disseminated and in the

exercise of the right to be forgotten.

The Constitutional Court

Thus, Sentence 107/1998 of the Constitutional Court specifies that:

"the preponderant value of the public liberties of art. 20 of the Constitution,

as soon as it is based on the function that these have of guaranteeing an opinion

public free public essential for the effective realization of political pluralism,

can only be protected when the freedoms are exercised in connection

with matters that are of general interest for the matters to which they refer and for

the people who intervene in them and contribute, consequently, to the

formation of public opinion, then reaching its maximum level of

justifying efficacy against the right to honor, which is weakened,

proportionally, as an external limit of the freedoms of expression and

information, insofar as its holders are public persons, they exercise functions

public or are involved in matters of public relevance, forced by

this to bear a certain risk that their subjective rights of the

personality are affected by opinions or information of interest

general, because political pluralism, tolerance and the spirit of

openness, without which there is no democratic society.

2) The political activity of the A.A.A. is not obsolete

(…)

Therefore, the disclosure was also adequate -according to the criteria established

in the aforementioned STS 1175/2020- taking into account the incidence of the time factor

in the quality of the data of the interested party disseminated and in the exercise of the right

forgotten.

3) The transparency question was related to his political activity.

(…)

What abounds in the justification of the knowledge that the question had its

origin in the context and environment of the referred party, when formulated by a person

linked to it.

Therefore, the publication of your personal data was justified from the

perspective also objective (in addition to subjective) according to the aforementioned STS

1175/2020.

4) Even if it was considered obsolete it should have been addressed to the search engine

Furthermore, even if A.A.A. is a former politician -what I know

contradicts not only the tenor of the question presented through the portal of

transparency, but with its permanence in the network with such a condition - should

having addressed, exercising the right, the search engine, not the CSIC as editor.

In this sense, the Judgment of the First Section of the Chamber of the

Contentious-Administrative of the National High Court dated February 5,

2015, in which the following was stated, in accordance with the Judgment of the

Court of Justice of the European Union of May 13, 2014 (Sentence

"Costeja" on the right to be forgotten), regarding a person who had

abandoned politics ten years ago (time elapsed substantially

higher than could be considered):

"The logical consequence is that whoever exercises the right of opposition must

indicate before the person in charge of the treatment, or before the Spanish Agency of

Data Protection, that the search has been made from your name

as a natural person, indicate the results or links obtained through the

search engine as well as the content of the information that affects it and that constitutes

a treatment of your personal data that is accessed through said

links, so that both the data controller and the

Agency itself has the necessary elements to carry out the trial

weighting referred to in the Judgment of the Court of Luxembourg; Thus

also deduces from article 35 of the Data Protection Regulation.

Thus, we proceed to apply the above to the assumption that we

occupies. B.B.B., exercised in April 2009 the right to oppose the treatment

of your personal data because when you enter your name in the search engine

Google appeared the reference to a web page of the Newsletter of the Community of

Madrid nº XXX, of ***DATE.1, in which the candidacies of the

municipal elections of ***DATE.2 of San Sebastián de los Reyes (Madrid).

Well then, said information lacks relevance that would justify that

prevail the interest of the general public of said personal data on the

rights recognized in articles 7 and 8 of the European Bill of Rights

Fundamentals. We are facing an initially lawful data processing by

part of the Google search engine that given the content of the information and the time

elapsed are not necessary in relation to the purposes for which they are

collected or treated.

On the other hand, freedom of information is satisfied by the

Subsistence at the source, that is, at the website where the information is published.

information, without the fact of removing from the list of results the links to

the web page object of claim by the affected party, prevents using other

data is reached to the aforementioned web page, but not from its name."

5) The identity has been suppressed

However, which, as stated in the letter of 10-20-2020, has been

proceeded, in response to the request transferred, to delete the reference to the

AAA identity as a requestor of information under the Law of

Transparency. What is developed in the next section.

Consequently, the insertion of identity in the context expressed

was correct as the identity and affiliation of the

claimant with a party, ***PARTY.1, involved in the issue of the

that the question was asked. A.A.A., even today, maintains inserts

linked to his political activity, so it was not obsolete.

All this without prejudice to proceeding and deciding its suppression with

precautionary character and in response to the request. “

On the Date on which it has been eliminated, the representatives of the claimed party have

manifested:

"Notwithstanding which proceeded, as stated, to consider the request and to

Take appropriate precautionary measures.

Documents with the filtered system logs for that file are attached. I know

can prove that as of 1:59:36 p.m. on February 1, when accessing the

web page, a 404 error was obtained, that is, the file had been

correctly removed from the CSIC website.

It is understood, on the other hand, that when there are consecutive accesses with

error the algorithms used by search engines, for example, Google, end up

deleting the reference to consider them obsolete.

Notwithstanding the foregoing, Google was requested to remove the URL from the cache. I know

attaches a document in which it is verified that, at least dated 11

February at 7:00 p.m., more than one request for annulment of the

URL of the cache, with the request appearing as a duplicate.

What the publisher cannot do is remove the reference and the cache from the servers of

the aforementioned company that follow the multinational's own programming that,

according to the transferred requirement, he remained on 2-10-2021."

They provide a copy of what appear to be log lines from the servers' log files

HTTP of the claimed, in which as of 13:49:52 on February 1, 2021

The error code 404 appears when accessing the cited pdf file. (At 1:49:51 p.m.

code 200 of no error or OK still appears).

They provide a copy of screenshots of Google Search Console where requested

to Google the withdrawal of the URL where it is found in pdf. on screen printing

indicates that the URLs of the search results are blocked and their

snippet and the cached version.

It has been verified that at the date of preparation of this report the

quoted pdf document in Google cache.

Information has been requested on the existence in your organization of a

written procedure for the anonymization of personal data of resolutions and

other documents that are published on the web. Information about whether

Procedures include actions to follow in case of errors. Information

on whether to consider possible indexing by search engines of personal data

published by mistake, as well as the elimination of these indexes both from the search engine and

of its possible cache. Copy of these procedures if so.

The defendant's representatives have stated:

“In this respect several circumstances must be signified.

a) anonymization criteria in the CSIC

The insertion of personal data on the CSIC website linked to projects does not

it is usual. A large part of the projects refer to research in non-living life.

human and matter, with the presence only of the data of the researchers

involved.

The most extensive processing of personal data at the CSIC

are those linked to the job market and calls. In this regard, since

years proceed as follows, applying the criteria of the

Seventh additional provision of Law 3/2018 on Data Protection

Personal and guarantee of digital rights:

Job Bank

The CSIC manages, through its Electronic Headquarters, multiple calls for

employment and training, as well as a job bank with thousands of applicants and

which gives rise to thousands of contracts each year, approximately 3,000 people.

The information of the Exchange that shows personal data is the one that appears in the

lists of merits, both provisional and definitive.

As an anonymization criterion in all lists of provisional merits and

definitive, as well as in the resolutions, it appears:

 Anonymized NIF: it only allows you to see four characters, the rest goes with

asterisks.

- The name and surnames are clear.

An example of a list of provisional merits is attached (file:

LP_GP12_10022021.pdf) and another of definitive merits (example:

LD_SOLAUT_36201.pdf).

calls

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

The CSIC manages different internal calls of different modalities,

JAES, Youth Guarantee and other types of positions.

In all the documents (lists of admitted, excluded, passed phases,

resolutions, etc.) appears the name and surname of the participants in the

announcement. The NIF never appears, which is replaced by the reference of your

application or contract to which they are presented, according to the modality of the call.

The headquarters shows very different types of list, according to the different phases of the

procedure, but in all of them the same criterion is followed: The NIF does not appear

but the Reference of the Request and yes the name and surname are shown.

A resolution is attached as an example.

b) instructions and organizational, coordination, information and support measures

workers and units for anonymization.

The CSIC is made up of 120 institutes and centres. Many of whom have

Web pages. The point of coordination in them are the managements.

For the articulation of data protection policies, specifically as regards

that refers to publication on the web pages, the Data Protection delegate

data has an authorization to send emails to all the managers of

the CSIC ICUs:

authorizedsldtger@listas.csic.es

Additionally, to the criteria transferred for each specific assumption to the

competent units in the sense exposed, there is a section

"data protection" on the CSIC intranet where accessible information appears

to the more than 11,000 workers of the center.

In it is inserted the following instruction that refers to

to the AEPD anonymization guide, as well as the Guide itself.

Information of a personal nature on the Web should be avoided if it is not

justified. It is understood as personal information the Names and

Surnames, DNI or Equivalent, Postal and Electronic Addresses, Telephones,

bills etc. of natural persons.

This circumstance reaches the possible improper identification of professionals

representatives The data of third parties professionally involved, the manager

of a company, the lawyer who represents etc. will also be anonymized

when its insertion is not justified. As well as numerical references,

codes of different types, which could allow the improper identification of a

Physical person.

This forces us to consider the set of criteria to be applied in the development of the

semi-automated anonymization tasks.

"the

xxxx

Spanish,

Juan Spanish

onwards

In the resolutions that are made public in which the circumstance of

the existence of a single affected party should opt for the standard of style

consisting of citing your anonymized identity only once:

"D.

affected/interested/complainant""

And avoid reproducing the name later. Sometimes that rule is introduced

style, but, despite everything, there is a risk of anonymization in the first

citation reproducing the name later.

The anonymization guidelines issued by the

Spanish Data Protection Agency:

https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-

anonymization-procedures.pdf

Special consideration must be given to what is contained in the Provision

additional seventh of the law 3/2018 of Protection of Personal Data and guarantee

of digital rights.

Seventh additional provision.

Identification of those interested in notifications through advertisements and publications of administrative acts.

When it is necessary to publish an administrative act containing personal data of the affected party, it will be identified by its name and surnames, adding four random numerical figures from the national document of identity, foreign identity number, passport or document equivalent. When the publication refers to a plurality of affected these random digits should alternate.

When it comes to notification through advertisements, particularly in the assumptions referred to in article 44 of Law 39/2015, of October 1, of Common Administrative Procedure of the Public Administrations, will identify the affected party exclusively by means of the complete number of his national identity document, foreigner identity number, passport or equivalent document.

When the affected party lacks any of the documents mentioned in the two previous paragraphs, the affected party will be identified only by his Name and surname.

In no case should the name and surnames be published jointly with the complete number of the national identity document, identity number of foreigner, passport or equivalent document.

In order to prevent risks for victims of gender violence, the Government will promote the development of a collaboration protocol that defines secure procedures for publication and notification of administrative acts, with the participation of the bodies with competence in the matter

For more

delegateprotecciondatos@csic.es

It should also be noted that both in the periodic meetings with the

managers, as well as with the other workers, especially again

information or clarification

contact

with

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

entry, a reminder is made regarding the obligation to anonymize

data when applicable.

In addition, the email of delegateprotecciondatos@csic.es can be found at

disposal of the staff, also for the purpose of inserting data on the web.

The DPO is involved as required and is consulted when there is any

issue on which doubts or problems may arise, such as the one raised,

having responded in 2020 to 75 questions or queries, all without prejudice to

activities undertaken on their own initiative and in other settings.

Such involvement is greater in procedures in which, in principle,

process data, such as calls and other resolutions of personnel or aid in

the stated meaning.

c) Procedures to detect errors

For the eventual detection of errors, an analysis of the files is carried out

indexed in search engines using specific software used

mainly to find metadata and hidden information in the

documents that it examines and that are published on the website.

The documents that are scanned are usually Microsoft files

Office, Open Office, or PDF files, and these documents are searched using

three possible search engines that are Google, Bing and DuckDuckGo.

It should be clarified that the content of the documents is not analyzed, but the

associated metadata, such as a personal email, a name, etc. I know

Attaches the generated report in which no sensitive metadata is detected in the

institutional website.

On the other hand, for October 2021 it is planned to carry out the biannual audit by

AENOR including website and headquarters. Attached is the current document with the

AENOR certification of compliance with the National Security Scheme. “

FIFTH: On September 1, 2021, the Director of the Spanish Agency for

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

for the alleged infringement of article 5.1.f) of the RGPD and article 32 of the RGPD,

typified in article 83.5 of the RGPD. Notified the start agreement, the claimed

presented a brief of allegations in which, in summary, it stated that the relevance

applicant's policy was to be considered with respect to the disclosure of her

identity, which meant that, in any case, its eventual disclosure was not

disproportionate, that the claimant's political activity was not obsolete, that the

transparency question was related to his political activity, which had been

proceeded to the suppression of the identity, that the measures of

necessary technical and organizational security that had been violated, that

In the present case, the figure of medial competition concurred since "an infraction is

a necessary means for the commission of another” and requested that the

exposed arguments and proceed to file the file

SIXTH: On November 16, 2021, a resolution proposal was formulated,

proposing:

the

<< That the Director of the Spanish Agency for Data Protection directs a

warning to

STATE AGENCY SUPERIOR COUNCIL OF

SCIENTIFIC INVESTIGATIONS, with NIF Q2818002D, for an infringement of the

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

classified as very serious for prescription purposes in article 72.1 i) of the

LOPDGDD and for violation of article 32 of the RGPD, in accordance with the provisions of the

article 83.4 of the aforementioned RGPD, qualified as serious for the purposes of prescription in the

Article 73 section f) of the LOPDGDD. >>

SEVENTH: On November 23, 2021, the respondent filed a brief of

allegations to the Motion for a Resolution, in which, in summary, it states that the

allegations have been partially analyzed and the arguments already

set forth in previous claims.

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

In this proceeding, the following are considered proven facts:

FACTS

FIRST: On August 15, 2020, the claimant filed a claim with

the Spanish Data Protection Agency, against the STATE AGENCY

SUPERIOR COUNCIL OF SCIENTIFIC RESEARCH, since the

defendant issued a resolution on his case allowing partial access to the

requested information, openly publishing the resolution, since, although

placed a black rectangle above his name and surnames, this text was not

deleted, and it appeared in the pdf, so it was possible to access and locate it

using an internet browser or pdf editor.

SECOND: It is verified that it is a pdf document in which, by performing a

search of the text finds an occurrence (one of one: 1/1), although said text

it is not displayed as it appears to be hidden with a black rectangle. It is verified that

can be extracted from this document, by copying and pasting, the text below the

black rectangle.

THIRD: On 02/10/2021, access to the URL address is attempted and verified

the page is no longer found. It is checked that using the search engine

from Google the text “A.A.A.” is still found. By accessing through the link

displayed by Google, the page post is not found. It is verified that the

The cited page is found in Google's cache.

FOUNDATIONS OF LAW

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

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

Director of the Spanish Data Protection Agency is competent to resolve

this procedure.

SECOND: In relation to the statements made by the claimed party,
basically reiterating the arguments already presented throughout the
sanctioning procedure, 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 first place, the fundamental right of the claimant, that their data not be
used in a surprising way, associated with the development of their task, suppose a use not
legitimate of said data, not adequate, necessary, or justified. must be taken into
Note that the data protection regulations do not make a distinction between data
public and private, allowing without further ado, the use of data that the affected party has made
public, but generally grants protection to personal data
determining those assumptions in which said treatment results in accordance with the
same.

The Constitutional Court comes to establish the right to data protection as
autonomous fundamental right. By virtue of this fundamental right, the citizen,
in general, you can decide on your own data.

In this sense, the jurisprudential doctrine of the Court must be taken into consideration.
Constitutional Law in this matter, which configures the right to data protection as
an autonomous fundamental right, differentiated from the fundamental right to
privacy. Thus, in its Judgment 292/2000, it states the following:

Thus, the object of protection of the fundamental right to protection
of data is not reduced only to the intimate data of the person, but to any type of
personal data, whether intimate or not, whose knowledge or use by third parties may
affect their rights, whether or not they are fundamental, because its purpose is not only the
individual privacy, which is the protection that art. 18.1 CE grants, but

personal data. Therefore, it also reaches those data

personal public, which, by virtue of being public, being accessible to the knowledge of

any, do not escape the power of disposition of the affected party because this is guaranteed by their

right to data protection. Also for this reason, the fact that the data is of a

personal does not mean that only those related to private or intimate life have protection

of the person, but the protected data are all those that identify or

allow the identification of the person, being able to serve for the preparation of their profile

ideological, racial, sexual, economic or of any other nature, or that serve to

any other utility that in certain circumstances constitutes a threat

for the individual."

The aforementioned Judgment 292/2000 also determines the content of the right to

protection of personal data indicating in its legal basis 7:

“From all that has been said, it follows that the content of the fundamental right to

data protection consists of a power of disposal and control over data

personal information that empowers the person to decide which of these data to provide to

a third party, be it the State or an individual, or what this third party can collect, and that

it also allows the individual to know who owns that personal data and for what,

being able to oppose that possession or use. These powers of disposition and control

on personal data, which constitute part of the content of the right

fundamental to data protection are legally specified in the power to

consent to the collection, obtaining and access to personal data, its subsequent

storage and treatment, as well as its use or possible uses, by a third party, be it the
State or an individual. And that right to consent to knowledge and treatment,
computerized or not, of the personal data, requires as complements
essential, on the one hand, the ability to know at all times who has
that personal data and to what use it is subjecting them, and, on the other hand, the power
object to such possession and uses.
Finally, they are characteristic elements of the constitutional definition of the right
fundamental to the protection of personal data the rights of the affected party to consent
about the collection and use of your personal data and to know about them. and they turn out
essential to make this content effective is the recognition of the right to be
informed of who owns your personal data and for what purpose, and the right to be able to
oppose such possession and use by requiring the appropriate party to put an end to the
possession and use of data. That is, demanding from the owner of the file that
Report what data you have about your person, accessing your appropriate records and
seats, and what destination they have had, which also reaches possible assignees; Y,
where appropriate, require him to rectify or cancel them."
The object of protection of the fundamental right to data protection is not reduced
ce only to the intimate data of the person, but to any type of personal data, whether or
non-intimate, whose knowledge or use by third parties may affect their rights,
whether fundamental or not, because its object is not only individual intimacy, which is already
would be protected by article 18.1 of the Constitution, but personal data
sound. That is to say, the TC comes to extend this fundamental right to personal data.
public, which by the fact of being public cannot escape the power of disposition
tion of the interested party or affected party, not being restricted to those related to private life.
or intimate information of the person, but the protected and protected data are all those
Those that identify or allow the identification of the person, that can configure

their ideological, racial, sexual, economic profile, etc.

The fundamental right to data protection is specified in a power of disposition

tion and control over personal data. In this way, the person must be

empowered to decide which of their data to provide to a third party, be it the Administration

transaction or an individual, decide which ones this third party can collect, know who owns

that personal data and for what, being able to oppose that possession or use.

This right, thus configured, requires as essential complements, the faculty

the right to know at all times who has these personal data and to what use

is submitting them, as well as being able to oppose that possession and uses.

Therefore, any action that involves depriving the person of those faculties

disposition and control over your personal data, will constitute an attack and a vulnerability

ration of their fundamental right to data protection. In this sense, it is pronounced

the TC, in Judgment 11/1981, of April 8, "the content is exceeded or unknown

essential when the right is subject to limitations that make it impracticable,

make it more difficult than reasonable or deprive it of the necessary protection".

Second, from the facts proven in this proceeding, it follows that

the entity complained of in its capacity as public body responsible for the treatment

of personal data should have adopted the necessary measures to prevent

any access to the personal information contained in said

documentation. Such measures were not fully adopted in this case,

as evidenced by the fact that the identification data appeared on its website

of the claimant in this proceeding.

Data anonymization should be considered as a way to eliminate the possibilities of personal identification. The advancement of technology and available information make it difficult to guarantee the anonymity. absolutely, especially over time, but, in any case, anonymization will offer greater guarantees of privacy to individuals.

In this sense, the use of measures such as, for example, the mechanisms and anonymization protocols that entail the definition of the work team, the staff training, confidentiality measures, the use of possible standards, the use of codes of good practice, etc., define explicit the intention and diligence of the data controller in the processes of anonymization of personal data.

However, it is verified that the conflicting document has been withdrawn from the this procedure, which shows that all the necessary steps were taken for prompt resolution of the problem.

The National Court, in several sentences, among others those dated February 14 and September 20, 2002 and April 13, 2005, requires entities that operate in the data market, special diligence when carrying out the use or treatment of such data or its transfer to third parties, since it is about the protection of a fundamental right of the people to whom the data refers, so the depositories of these must be especially diligent and careful when it comes to carry out operations with them and must always opt for the most favorable to the protection of the legal rights protected by the norm.

Lastly, article 29.5 of Law 40/2015 refers to what is known as “con-medial course of administrative infractions”, which is applicable when an infraction lighter fraction serves as a means to commit a more serious one. For it to result from

application, it is necessary to verify the concurrence of a plurality of actions

which, in turn, give rise to a plurality of infractions (for example, two

chos and two infractions); with the particularity that one of them is an instrument or

means necessary for the perpetration of the other.

In accordance with the previous fundamentals, it is clear that an action has taken place,

the violation of the security of data processing by not anonymizing them

properly, which has resulted in a violation of result by

their loss of confidentiality. Since several actions do not concur, there is no

before a “medial insolvency”, nor can the aforementioned article 29.5 be applied to the case.

Consequently, the allegations must be dismissed, meaning that the

arguments presented do not distort the essential content of the infraction that

declared to have been committed, nor do they imply sufficient cause for justification or exculpation.

The defendant is accused of committing an infraction for violation of the

article 5.1.f) of the RGPD, which governs the principle of confidentiality and integrity of the

personal data, as well as the proactive responsibility of the data controller

treatment to demonstrate compliance and article 32 of the RGPD.

THIRD: Article 5.1. f) of the RGPD that establishes:

"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 ("integrity and confidentiality").

In this way, the exposure on the website of the defendant gives rise to the rupture of the

confidentiality bond of the data controller.

Article 5 of the LOPDGDD, Duty of confidentiality, states the following:

"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 to the

duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will be maintained even when

the relationship between the obligor and the person in charge or in charge of the transaction had ended.

treatment".

FOURTH: Regarding the security of personal data, 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 account shall be taken of

takes 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 person in charge or the person in charge and

has access to personal data can only process said data following

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

the Union or the Member States.

It should be noted that the RGPD in the aforementioned precept does not establish a list of the

security measures that are applicable according to the data that are subject

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 technical measures and organizational must be carried out taking into account: pseudonymization and encryption, capacity to guarantee confidentiality, integrity, availability and resilience, the ability to restore availability and access to data after an incident, process verification (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.
The liability of the claimed party is determined by the security breach
revealed by the claimant, since he is responsible for making decisions
aimed at effectively implementing the technical and organizational measures
appropriate to guarantee a level of security appropriate to the risk to ensure the
confidentiality of the data, restoring its availability and preventing access to the
in the event of a physical or technical incident.
FIFTH: Article 83.5 of the RGPD provides the following:
"5. Violations of the following provisions will be sanctioned, in accordance with the
paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or,
in the case of a company, an amount equivalent to a maximum of 4% of the
global total annual turnover of the previous financial year, opting for
the largest amount:
a)
basic principles for treatment, including conditions for con-
sentiment under articles 5, 6, 7 and 9;"
For its part, article 71 of the LOPDGDD, under the heading "Infringements" determines what
following: Violations constitute the acts and conducts referred to in the
sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.

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

under the rubric of infractions considered very serious, it establishes the following:

"1. 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:

(…)

Yo)

The violation of the duty of confidentiality established in article 5 of

this organic law.

The violation of article 32 RGPD is typified in article 83.4.a) of the

cited RGPD in the following terms:

"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 83.5 and 83.4 of the GDPR, transcribed above.

SIXTH: Establishes Law 40/2015, of October 1, on the Legal Regime of the Sector Public, in Chapter III regarding the "Principles of the sanctioning entity", in the article 28 under the heading "Responsibility", the following:

"1. They may only be sanctioned for acts constituting an administrative infraction. natural and legal persons, as well as, when a Law recognizes their capacity to to act, the affected groups, the unions and entities without legal personality and the independent or autonomous estates, which are responsible for them title of fraud or guilt.”

Lack of diligence in implementing appropriate security measures with the consequence of breaching the principle of confidentiality constitutes the element of guilt.

SEVENTH: Article 58.2 of the RGPD, states the following:

2. Each control authority will have all of the following corrective powers in-

listed below:

(…)

“b) send a warning to any person responsible or in charge of the treatment when

treatment operations have infringed the provisions of these Regulations.

unto.”

For its part, the Spanish legal system has chosen not to penalize

imposition of an administrative fine on public entities but with a warning, such

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 issue a resolution

sanctioning them with a warning. The resolution will also establish the

measures to be taken to stop the conduct or correct the effects of the

offense 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 corresponding Official State or Autonomous Gazette

4. The data protection authority must be notified of the resolutions that fall in relation to the measures and actions referred to in the sections previous.

5. They will be communicated to the Ombudsman or, where appropriate, to 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 responsible or in charge of the treatment that had committed the infraction."

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

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

Spanish Data Protection Agency RESOLVES:

FIRST: SANCTION WITH A WARNING the STATE AGENCY

SUPERIOR COUNCIL OF SCIENTIFIC RESEARCH, with NIF Q2818002D,

for an infringement of article 5.1.f) of the RGPD and article 32 of the RGPD, typified

in articles 83.5 of the RGPD and 83.4 of the RGPD, respectively.

SECOND: NOTIFY this resolution to the STATE AGENCY COUNCIL

SUPERIOR OF SCIENTIFIC RESEARCH.

THIRD: 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

938-231221

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es