 File No.: PS/00028/2022

RESOLUTION OF SANCTIONING PROCEDURE

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

the following

BACKGROUND

A.A.A., (hereinafter, the claimant) on 03/31/2021 filed

FIRST:

claim before the Spanish Data Protection Agency. The claim is directed

against GETAFE CITY COUNCIL with NIF P2806500A (hereinafter, the defendant).

The reasons on which the claim is based are the following:

The claimant points out that by accessing the alleged

document "***DOCUMENTO.1 Resolution calling for an extraordinary meeting of the

Full Town Hall to celebrate *** DATE.1"

points to an excel file

), "which once opened,

https://sede.getafe.es/portalGetafe/sede/RecursosWeb/

contains names and surnames, address, IDs, dates of birth and license plates and date

vehicle registration."

He also states that he has filed a complaint for this reason against the defendant himself.

03/31/2021, provide a copy.

(...)

Although there are 36 records, the vast majority are repeated once or twice, in total: (...)

people

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5/12, of

Protection of Personal Data and guarantee of digital rights (hereinafter

LOPDGDD), transfer was made on *** DATE.2 of said claim to the defendant

within the framework of procedure E/04923/2021, to proceed with its analysis and

inform this Agency within a month of various issues. In the shipment

informed of the exposed document and the URL that hosted the file and requested various

information.

There is no response to the transfer, which was notified electronically, stating: "date

of acceptance: 05/04/2021 12:34:05".

THIRD: On 06/31/2021, by application of article 65.5 of the

LOPDGDD, the processing of the claim continues.

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

preliminary investigation actions to clarify the facts in question,

by virtue of the investigative powers granted to the supervisory authorities in the

Article 57.1 of Regulation (EU) 2016/679 (General Regulation for the Protection of

Data, hereinafter GDPR), and in accordance with the provisions of Title VII, Chapter

I, Second Section, of the LOPDGDD, being aware of the following points:

-Dated 09/10/2021, the AEPD sent a request for information via

electronically in order to obtain more detail on the facts claimed. According to

report of the "Service of Electronic Notifications and Electronic Address Enabled

of the FNMT-RCM", dated ***DATE.3, the automatic rejection of the

requirement, after ten calendar days have elapsed since it was made available.

On ***DATE.4, the previous request is reiterated, this time by post.

This time, as evidenced by the confirmation of receipt of the notification issued by

the “Citizen Folder” application, the defendant accessed it on ***DATE.4.

The request was not dealt with within the time allowed.

-On 12/1/2021, access to the section corresponding to the "Consultation of Records of

Plenary Sessions" of the electronic headquarters of the claimed party. Within the list of sessions, consult

the one corresponding to ***DATE.1 as it is the one referred to by the claimant. The result

of this evidence, incorporated into the file through the "References Diligence", does not

redirects to the list referred to by the claimant, but to the effective call of the aforementioned

plenary, (https://sede.getafe.es/portalGetafe/sede/RecursosWeb/(...)).

of

data

aforementioned

list

-Next, on the same day 1/12, you access directly through the browser to the

electronic address provided by the claimant in which he supposedly joined

he

personal,

https://sede.getafe.es/portalGetafe/sede/RecursosWeb/(....) and download the "excel sheet"

to which one has access and is incorporated as an associated object of the file. "Given the

The SIGRID system does not allow the incorporation of documents in Excel as annexes to

the proceedings, it is converted to pdf format and attached to this proceeding. The sheet,

titled "FEMP Agreement Request" in which thirty-six records are listed with the

following fields: "Code", "Name", "Surname 1", "Surname 2", "Doc_Identifier" NIF,

“Date_Birth”, “Type_Vía”, “Nombre_Vía”, “Nº”, “Block”, “Gateway”, “Stairs”,

“Plant”, “Door”, “Km”, “Hm”, “Town”, “Postal_Code”, “Record Type”, “License Plate”,

"Date_Matriculation", "Co-owners", "Impression", "Observations", "Date_Resolution",

“Resolution”, “Description”. The personal data that appears to appear in said list

are: name, surname, address, date of birth, tax identification number,

NIE, vehicle registration, and registration date.

FIFTH: On 01/25/2022, a letter was received from the defendant, which stated in

response to information request E/7831/2021:

"This entity has not sent the information within the required period, given that in said

-

period there was a transition of responsibilities in terms of data protection

between the Information Security Committee, a consultative and strategic body for the

decision-making in matters of Information Security, and the current Delegate of

Data Protection whose inauguration took place on 10/1/2021”.

-On 03/31/2021, at the municipal electronic headquarters, area corresponding to the bulletin board

announcements and electronic edicts, we proceeded to publish from the unit of

*** DEPARTMENT.1, a content referred to the Resolution of the meeting call

extraordinary session of the City Council, Plenary, to be held on ***DATE.1. Due

of a human, involuntary and accidental error, the incorrect information resource was attached,

and instead of attaching the pdf corresponding to the aforementioned resolution, a sheet was attached

internal and temporary calculation in which identification and personal data of

(...) citizens. The compromised data are "name, surname, ID, postal address".

“The information that could have been accessed by third parties could cause damage to

those affected, but initially no serious harm is observed.”

Upon receiving a complaint that day, that same day, which was the same day of publication, it was corrected from ***DEPARTMENT.1 with the withdrawal of the document and the correction of the incident. On 04/22/2021, a response to the complaint was sent, deeming the case closed. proceedings.

-Regarding the actions taken to solve the incident and minimize its impact,

states that he himself (...), replaced the excel document with the pdf document of the extraordinary session of the City Council.

Since the publication of content is decentralized, a letter was sent reminder to the finalist units in which they are urged to carry out a "cross review" peers, thus ensuring that each publication is reviewed by a person from the Department other than the one that performs the update or publication on the website or headquarters municipal corporate.

-Regarding the security measures of the processing of personal data adopted prior to the incident, states:

a) Those contained in annex two of security measures of Royal Decree 3/2010 of 8/01, which regulates the National Security Scheme (ENS) in the field of electronic administration.

b) In the field of content management and publication:

-Management application managed according to profiles and departments.

-The contents to be published are made in PDF support according to the “corporate publication instruction”.

-Published, unpublished and restricted content is available with "access logs".

It adds that the incident is an error in a manual procedure which prevents its repetition for reasons of automation.

-The activity of processing personal data and called ELECTRONIC HEADQUARTERS,

Given the nature of the data, scope, context and purposes, it has been considered that it is not

entails a high risk for the rights and freedoms of natural persons, for which reason

There is no impact assessment study in terms of Data Protection.

Provide a copy of the record of processing activities SEDE ELECTRÓNICA.

-As for whether the security breach was notified to those affected, it states that the

same day that the situation became known, which was the day of the publication of the

content, the correction of the incident was made and the notification of the

situation to those affected,

-As for whether the security breach has been notified to the control authority before

that 72 hours had elapsed since it happened, he states that he did not send

information in that period, given that in that period there was a transition from

responsibilities in terms of Data Protection between the "Committee on security of the

information", an advisory and strategic body for decision-making in matters of

information security and the current "Data Protection Officer" whose decision making

Possession took place on 10/1/2021. It also notes that "information that may have

been accessed by third parties could cause harm to those affected, but initially

no serious damage is observed."

-Regarding the measures adopted so that a similar incident does not occur again

in the future, states that they have updated the content publication instruction

corporate, urging the units to carry out the "cross review".

Finally, they state that at the time of writing this report, the Department of

informatics has reviewed all the information content stored and published both in the

web as in the municipal headquarters, not having found any resource or in which

content contains personal data.

SIXTH: On 04/04/2022, the Director of the AEPD agreed:

"FIRST: INITIATE SANCTION PROCEDURE for the CITY COUNCIL OF

GETAFE, with NIF P2806500A, for alleged violations of the GDPR, articles:

-5.1.f), in accordance with article 83.5.a) of the GDPR, typified in article 72.1 a)

of the LOPDGDD.

-32, in accordance with article 83.4.a) of the GDPR, typified in article 73.f) of

the LOPDGDD.

-33, in accordance with article 83.4.a) of the GDPR, typified in article 73.r) of the

LOPDGDD."

"… For the purposes specified in the art. 64.2 b) of Law 39/2015, of 1/10, on Procedure

Common Administrative Law of Public Administrations, the sanction that could

to correspond would be a warning, without prejudice to what results from the instruction."

Once the agreement was received, no allegations were presented.

SEVENTH: On 06/23/2022, a test practice period begins, assuming that

reproduced for evidentiary purposes, the claim filed and its documentation, the

documents obtained and generated during the admission process phase of the

claim, and the report of actions that are part of the procedure

E/07831/2021.

Likewise, it is considered reproduced for evidentiary purposes, the allegations to the

initiation of the aforementioned sanctioning procedure,

presented by the defendant and the documentation that accompanies them.

The claimant is requested to report or provide the following information for verification

and verification of the existing measures at the time of the events:

a) In the report of previous actions, it appears that "On 12/1/2021, it is accessed by the

pector in the phase of actions prior to the section corresponding to the "Consultation of Ac-

Plenary Sessions" of the electronic headquarters of the claimed party. Within the list of sessions,

check the one corresponding to ***DATE.1. The result of this test, incorporated

to the file through the "References Diligence" does not redirect to the list referred to by

the claimant but to the effective convocation of the aforementioned plenary session.

Then, on the same day 1/12, you access directly through the browser to the

email address provided by the claimant https://sede.getafe.es/portalGetafe/sede/

WebResources/(...). The result of this test, incorporated into the file through the

"References Diligence", is access to a document in Excel format that contains

a sheet entitled "FEMPAgreement Request" The personal data that seems to be noticed

in said list are: name, surname, address, date of birth, identification number,

tax identification, vehicle registration, and date of registration."

It is requested to explain the reason why they did not verify the access from the url in navigation.

(after indicating that upon receiving the complaint (...) they solved the matter), considering that the

12/1/2021 the inspector again accessed the content of the list by typing in the browser

gador the address originally obtained by the claimant (https://sede.getafe.es/

portalGetafe/sede/RecursosWeb/(...).

On 07/07/2022, the defendant states that "the content was accessible

from the area of the web called "consultations of plenary minutes" but also in "ta-

billboard". "The specific publication of the content of the Extraordinary Call

of the Plenary Session dated ***DATE.1, was held from the ***DEPARTMENT-

TO.2, who is in charge of publishing these contents on the "Notice Board"

Municipal in electronic Headquarters.

"Once the complaint was received, the processing and response to it was carried out by the

unit of ***DEPARTMENT.1 (unit responsible for the content (...). This unit re-

sent the request for the deletion of the information to ***DEPARTMENT.2, unit that

unlinked the content object of complaint and that linked the correct content and referring to

the call for the session in PDF format. Upon receipt of the reply in ***DE-

DEPARTMENT.1 by ***DEPARTMENT.2 with the communication of the correctness

of the incident, he verified (making only use of the navigation options)

the portal, the effective absence of said content), thus closing the incident.

cia and issuing the response to the complaint, thus closing the file."

"In the resolution of the complaint, two units not specialized in the management

of contents, so that the effective verification of the deletion by accessing the URL

it was not done."

a) Proof of the date on which access is withdrawn or disabled through the browser.

dor, from https://sede.getafe.es/portalGetafe/sede/RecursosWeb/(...).

"The document was deleted on 01/24/2022, with the intervention of the Information Unit.

format, verifying the content of the URL, and the elimination of the aforementioned worksheet

calculation in the municipal content manager, moment in which the training was carried out and

explanation of what happened to this unit and to the resources in charge of using the manager

of contents. The technical detail of what happened is that the record was not deleted.

course, but rather disassociated himself from the documentary to which he found himself related, in a

so that the document was "orphaned" in the manager, and therefore, although it was not accessed

ble following the navigation route in the portal, if from the URL and therefore internet

."

“We proceeded to carry out an “in situ” training as well as to carry out by Protection

of Data an instruction that operationally improves the guarantees in the publication phase.

tion of contents, especially those that are especially sensitive, such as those that contain

They have personal data. This instruction is applicable both in the publication of content

municipal website as well as those of the headquarters”.

b) Inform about the details of the list, what was it used for?, on what date was it made?

mentioned and up to what date is it kept? What unit managed it? If the data were ceded?

to another unit(s)?, and if these data had to be published for some reason to the public?

co? or if it was a work file, who could be communicated to?

It states that "The list is a temporary work document in which the

part of ***DEPARTMENT.2 all the data referring to requests for change of

addresses of vehicle owners, and whose starting information is the requests received

registered in the General Municipal Entry Register (both in person

as electronics). The date of preparation of the document corresponds to the week of

the publication since the code of the input records determines the temporality of the

same. This file is prepared weekly and its purpose is to send it directly to the

Provincial Traffic Headquarters and is deleted once you have the ok of the upload process.

ga of said entity. The initial template was provided by the Traffic Headquarters,

may contain elements such as the creation date as metadata, which do not correspond to

corresponds to 2020. The entity that processes and manages this document is the same one that published

by mistake, ***DEPARTMENT.2.”

c) Structure of the electronic headquarters regarding the publication of documents with data

personal, what documents have to be exposed, in what section.?

Provides a screen print of "welcome to the electronic office" including the section

"procedures and records" headed by "procedures catalog", in the "Services" section is-

tá: "Virtual office", "electronic applications", "payments receipts" "self-assessments, taxes

and payments", "issuance of documents", "prior appointment" and "Personal Office". In the apart-

do: "You may be interested", includes, among others, the section on consultations and Plenary Sessions, Ac-

government boards. On the right side there are thematic tabs such as "profile

of the contracting party" "transparency portal", "bulletin board".

The defendant exposes the spaces where there may be personal data. Add

that there are contents and services that require prior identification.

d) Which unit is in charge of exposing the calls to the public at the headquarters?

of sessions of the Plenary City Council?, and if within said unit the same person always does it?

person and whether that person or persons have received training on protection or insti-

struction of the corporate data publication protocol, or written instructions if the

there is about the work to be done. The same for the unit that managed the document

Listing sheet titled "FEMPAgreement Request".

Answer that the publication of calls is made by two units, ***DEPAR-

TAMENTO.1 that publishes the plenary minutes at the headquarters, in "consultations of minutes of Ple-

nos", ***DEPARTAMENTO.2, which is also published at headquarters, on the "bulletin board".

They appear published in both areas. (...), indicating that all people have received

do training on data protection.

On the existence of an instruction or protocol for the protection of classified cargo data.

tion and publication of content, answers that "yes, initially there was a ma-

manual, guide and procedure for uploading, classifying and publishing content, and post-

Prior to the incident, an instruction was drawn up urging a cross-review

between equals, thus ensuring that each publication is reviewed by a person from the

department other than the one that performs the update/publishing on the web / corporate headquarters

rative. - All these data apply to both units."

e) Regarding the sheet titled: "FEMP Agreement Request" that contained the list of the

(...) people, what relationship existed between the people with that administration so that

The personal data will appear in said records, what type of relationship or activity relates to them.

did it work?

They stated that they are owners of vehicles registered in the municipality and that they have requested

change of address, the category of data is "citizens".

f) Record of processing activities applicable to the list sheet titled "RequestCon-

venioFEMP", and reasons that justify the treatment of NIF, name and surname, registration

vehicle, address.

The treatment activity to which it corresponds is: "General Registry", whose purpose is

the Record of Entry and Exit of documents and referral to the municipal department

authority, as well as "Queries and Information on documents, procedures, tra-

mites or notifications and communications from the City Council". It provides details of the registry of

treatment. The elements that are treated are necessary for the Provincial Headquarters of

Traffic that receives the data and determined the format, order, and content of the cells in the

sheet.

g) If they made a documented assessment of the impact on the confidentiality of the

people on the list and their rights and what technical and organizational security measures

on those data were applied.

It reiterates that "The information that could have been accessed by third parties could cause

cause damage to those affected, but initially no serious harm is observed."

Regarding the measures they have, in terms of content publication management:

- Managed management application according to profiles and departments.

- The contents to be published are made in PDF support, and in accordance with the "corresponding instruction"

publication policy" and "support manuals" developed by type of information or

service.

Provide screen print of "detail supplementary publication instruction to

all corporate manuals", "note for the publication of contents from the Management

corporate tor".

h) Documents generated and saved on the correction and incidence carried out by the

(...) related to data protection, time the sheet was published, if possible

It is possible to know how many views of the file or how many times the file was accessed.

Provide the entry documents, the internal certification of content removal, and the

report of 01/24/2022 REF ***REFERENCE.1, as well as the communication email to all

give the units reporting on the detail of the new publication instruction of

web content and municipal headquarters.

It states that the document that is the subject of the complaint is published on (...), there is a first

mere separation in that same file, with elimination of 01/24/2022, without distributing

Enter the number of views or accesses to the file.

i) Provide what they call: "the corporate publication instruction" in force at the time.

ment of the facts and their updates and explain why if in the protocol that you have

nian for the management of content publication had to be done in pdf, the applica-

tion supported appending an excel type?

It indicates that in Excel format it is not used for publications in headquarters, web, although the

application if it supports that format, without it being possible to restrict it to adapt it only to ad-

pdf mission. “Currently, a tool with more than ten years of experience is used.

antiquity”, adding that in September the headquarters will be updated with the use of a

most current content manager and improvements in content publication security.

It provides printing on the sheet as "detail complementary instruction to the manuals

corporatives” that contains the notes for the publication of contents in the administrative manager

nistrative

It provides as annexes 1 to 3, user manuals and "note for the publication of contents

from the corporate manager”.

j) In his letter he indicated that the "publishing of contents is decentralized",

Specify if there is not a unit that centralizes the instructions of the publication-exposure

for the questions of what data is exposed, what types of documents from each department

time can or have to be published, which are mandatory publication?

It states that "currently there is no unit that centralizes the instructions of the

publication / exposure for the questions of what data is exposed. The instruction

Operation developed after the incident was carried out by the Protection of

Data. Indicate that there is a municipal data governance strategy and promotion of

unique data, where one of the questions that arises is the creation of a Unit of

Organization and Data Management”.

k) In your response, you indicate that the current DPD took office on 10/1/2021, inform if in

At the time the events occurred, (...), there was no DPD and what role did it assume in the re-

clamation.

It states that this task was assumed by the Information Security Committee, which

did not intervene, since the processing of the incident was carried out in accordance with the procedure

management of suggestions and complaints.

l)

Documentation of the analysis that the breach is likely to constitute a

risk to the rights and freedoms of people when the NIF is known together or

NIE, name and surname, address and vehicle registration.

The data was published and linked at headquarters, one day, "the rest of the time

remained a difficult document to locate and consult", "as well as given the

volume of those affected initially assessed that the information that could have been

accessed by third parties, despite being able to cause harm to those affected, does not

I saw serious damage."

Attach annex 1, course minutes and plenary sessions and Governing Board in the electronic headquarters at

through the "Administrative web content manager", annex two, "board course

announcements of the electronic headquarters", in annex three, "notes for the publication of contents

from the corporate manager".

EIGHTH: On 10/28/2022, a proposal for a resolution of the literal was issued:

"That by the Director of the Spanish Agency for Data Protection be sanctioned with

warning to GETAFE CITY COUNCIL, with NIF P2806500A, for the following

GDPR violations:

- Article 5.1.f) of the GDPR.

- Article 32 of the GDPR.

- Article 33 of the GDPR.”

NINTH: On 11/17/2022, the defendant's allegations are received, requesting the

file of proceedings, stating:

1) The data contained in the files respond to a Collaboration Agreement

between the FEMP and the DGT for the modification of driving and circulation licenses

of vehicles, by change of domicile, which aims to facilitate this process for

citizens, as indicated on the website that reviews the DGT and the FEMP.

Said DGT website informs that the Agreement allows such changes to be made

directly in the offices of the Town Halls subscribed to the Agreement Add the

claimed that the structure of the document is used by numerous Town Halls.

2) The wrong document was only there for a few hours, it was replaced by the correct one the same

(…). The URL that the claimant had from his initial access and from which if possible

access was provided to the AEPD, it was the only means of accessing its content, therefore

that from the first moment, by normal technical means, the

document, unless the specific URL was available. The confidentiality of the data

published that could be affected was minimal, considering that "it is possible to think that the

claimant was the only one who accessed the data from the list that he provided", and this is how it is collected

in the proposal: "the claimant was at least able to access the data on the list that

contributed”.

The start agreement of 04/04/2022, was due to the persistence of the gap as indicated in the proposal, when what is true and so is given in proven facts, is that it points out, in According to the document of 01/25/2022 of the defendant, a detailed report was contained with the actions carried out, which included the elimination of the content manager of the electronic headquarters of the Excel file, explaining the cause that motivated the erroneous publication, and improvements in procedures. Therefore, consider that it is missing motivation in the opening of the procedure.

3) There is no evidence that the AEPD states that the claimant is affected by the treatment or that it has been part of the process. Still, the Agency continued processing his complaint despite the fact that the facts were resolved and that he lacks evidence on the real affectation to the rights of the affected persons. The claimant is not interested, the data processed does not concern him, starting the file by complaint from a third party, initiation of a procedure not provided for in the GDPR.

"We do not share the assessment of the AEPD on the infringement due to lack of

4)

communication of the security breach based on excessive data processing in within the framework of an Agreement with the DGT, without proof that the data processed They are excessive in relation to their purpose".

5) On the basis of law on the infraction due to lack of communication of the security breach to the authority, article 33 of the GDPR, indicating that it can "affect rights and freedoms, which advises that regardless of whether they have been produced damages to those affected and of the type that this may be, the authority is notified.", is qualified by the defendant as:

-conjecture, by not providing the AEPD with proof of what could have occurred in the event of that someone had accessed the data, and according to the proven facts, only a person agreed. The gap does not present a risk, since it was considered that it

damages were likely.

-No evidence is provided about what could have occurred in the event that some

person had access to the data. The constitutive facts of the

infringement or respect the presumption of non-existence of responsibility.

-In relation to the alleged infringement of article 32 of the GDPR, there were

organizational measures to mitigate the risks in the treatment. the publication

responds to a residual risk caused by human error. "There will always be a

inherent or initial risk and implicit in any treatment and, once they have been

measures and guarantees have been applied that minimize it, there will continue to be a residual risk".

It alludes to the judgment of the Supreme Court, no. 188/2022 third room, room of the

administrative litigation of 02/15, and exposes the theses of the obligations of

results and means included in the sentence.

PROVEN FACTS

1) The claimant. when accessing the electronic headquarters of the claimant to see a

call a plenary session, access the document "***DOCUMENTO.1 Resolution of

call for an extraordinary session of the Plenary City Council to celebrate the

***DATE.1", containing a list of personal data in excel format (address

electronic https://sede.getafe.es/portalGetafe/sede/RecursosWeb/(...)).

Once

open, contains personal data such as name, surname, address, date of birth,

tax identification number, NIE, vehicle registration, and registration date.

The complainant brings the facts to the attention of the defendant through a complaint

filed at (…), 1:44 p.m. and on the same date filed a claim with the AEPD.

2) According to the defendant, the specific publication of the content of the Call

Extraordinary Session of the Plenary Session dated ***DATE.1, was held on (...) from its

***DEPARTAMENTO.2, which is in charge of publishing these contents in the "Ta-

municipal Announcements blón in electronic office. The content that is the subject of the claim

it could be seen both in consultation of "plenum minutes" and in the "bulletin board".

3) According to what was stated by the defendant, the document object of the claim-

information that could be accessed by the claimant, in the electronic headquarters, the same

mo day that the claimant accesses, on (...) in two different sites of the electronic headquarters, in

"consultation of minutes of plenary sessions", and in "bulletin board". The defendant, upon receiving the claim

the same (...), proceeded to rectify it, replacing it with the pdf document co-

rresponsive. ***DEPARTMENT.1 checked the correctness only from options of

portal navigation

*** DEPARTMENT.1 processed the response to the claimant's claim and urged the

*** DEPARTMENT.2, your correction. ***DEPARTMENT.1 verified that the

corrected and the correct document had been exposed, on the same day (...), without verifying the

cash removed from the url via the browser.

4) On 12/1/2021, it was accessed by the AEPD inspector in the phase of pre-actions

via the section corresponding to the "Consultation of Plenary Minutes" of the electronic headquarters

ca of the claimed Within the list of sessions, consult the one corresponding to the day

***DATE.1. The result of this test, incorporated into the file through the "Dili-

Agency References" does not redirect to the list referred by the claimant, but to the effective

convocation of the aforementioned plenary session.

Then, on the same day 12/1/2021, it is accessed directly through the browser

to the electronic address provided by the claimant https://sede.getafe.es/portalGetafe/

headquarters/WebResources/(...). The result of this test, incorporated into the file through

of the "References Diligence", is the access to a document in Excel format that contains

There is a sheet entitled "FEMPAgreement Request". The personal data that make up di-

These lists are: name, surname, address, date of birth, identification number,

tax identification, vehicle registration, and registration date and coincides with that provided by

the claimant in his claim.

He explains that what happened regarding the appearance of the list in the browser was due to the fact that

left the document in the content manager with which it develops this function, it

linked from the link to which it was originally linked, but the resource was not deleted,

it being possible to access the route from the URL and that is why it appeared on the internet.

5) The defendant stated that the publication of content, in this case the call

of a plenary session, is carried out by two units, ***DEPARTMENT.1 that publishes at the headquarters

the minutes of plenary sessions, and ***DEPARTMENT.2 that also publishes at the headquarters, in the tab-

bulletin board (...), indicating that all people have received training on

data protection, there are written instructions that are given in courses for the

management of the publication of content resources.

6) The document object of the claim to which the Inspector of the AEPD was able to access the

12/1/2021 through the browser, it was deleted from it on 01/24/2022, it does not feel

do already accessible on the internet.

By correcting the URL in the browser, an instruction was approved that improves

operatively the guarantees in the publication phase of personal data content

them. This instruction is applicable both in the publication of municipal web content

as in those of the headquarters.

7) The document that the claimant was able to access is a working document that was

sent every week by the claimed to the Provincial Traffic Headquarters as a result of

an Agreement with the Spanish Federation of Municipalities and Provinces, to facilitate the

citizens that the change of address procedure can be carried out at the municipal office.

The document is processed by ***DEPARTMENT.2 of the claimant, same entity

that originally exposed it in the electronic headquarters when the claimant agreed.

8) The record of treatment that is applied to the data object of the claim is that of

"General Register".

9) The defendant provided for the management of content publication:

- The contents to be published are made in PDF support, and in accordance with the corresponding instruction.

publication purpose and support manuals developed, by type of information or

service, although the one that was uploaded was Excel.

- Management application, administered according to profiles and departments, in this case, the

Plenary summons is published by ***DEPARTMENT.2, one of the two Departments

cough enabled.

Provide screen print of “detail supplementary publication instruction to

all corporate manuals”, “note for the publication of contents from the Management

corporate tor”.

10) As actions taken as a result of the claim, a note has been added to

the instructions for the publication of contents, so that it is taken into account in the

corporate content manager in which "Data Protection" participated, was carried out

a formation of the case and a cross-review of what is published in the

headquarters or on the web, "by another person from the same department".

11) The defendant did not consider it appropriate to notify those affected because the same day of his

publication removed the content from the headquarters and on the permanence in the browser, ma-

It shows that the search needed to enter the specific URL, when (...) no fi-

was at the headquarters because it was eliminated, however, accrediting the certainty of power

have accessed while you have remained, that is, until 01/24/2022.

FUNDAMENTALS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter GDPR), grants each

control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the Law

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

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 Data Protection Agency will be governed by the provisions

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

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures."

II

In the present case, in accordance with the provisions of article 4.1 of the GDPR, the

processing of personal data, since the defendant performs the

collection, registration, access, use of personal data of natural persons, such

such as: name, identification number, etc. as accredited from the Excel file to which

the claimant had access.

The defendant carries out this activity in his capacity as data controller, given

who is the one who determines the purposes and means of such activity, by virtue of article 4.7 of the

GDPR.

Article 4 paragraph 12 of the GDPR defines, in a broad way, "violations of

security of personal data" (hereinafter security breach) as "all

those security violations that cause the destruction, loss or alteration

accidental or unlawful personal data transmitted, stored or otherwise processed

form, or unauthorized communication or access to said data."

In the present case, there is a personal data security breach in the

circumstances indicated above, categorized as a breach of confidentiality;

consequence of the exposure in electronic headquarters of an indexed file that is not

corresponded to what was claimed, and that it contained personal data. The process to take it

In effect, it is a process of human intervention that had its own protocol and was

developed with a corporate content manager as a tool to bring it to life.

effect.

It should be noted that the identification of a security breach does not imply the imposition

of a sanction directly by this Agency, since it is necessary to analyze the

diligence of managers and managers and security measures applied.

Articles 32, 33 and 34 of the GDPR, regulate the security of the treatment, the notification

of a violation of the security of personal data to the control authority, as well as

as the communication to the interested party, respectively.

II

Article 5.1.f) of the GDPR

The defendant is accused of a violation of article 5.1.f) "Principles relating to the

treatment" of the GDPR that establishes:

"1. Personal data will be:

(…)

f) processed in such a way as to guarantee adequate data security

personal data, including protection against unauthorized or unlawful processing and against their

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

appropriate organizational procedures (“integrity and confidentiality”).”

In this case, it is proven that there has been unauthorized access to

the personal data of the members of the Excel-type file that the claimant put in

its electronic headquarters, to which the claimant had access and which was kept in the browser,

violating the principle of confidentiality. The AEPD verifies that at least

12/1/2021, it is still possible to access the content by typing the email address in

the Navigator.

In accordance with the available evidence, it is considered that the facts

known are constitutive of an infraction, attributable to the defendant, for violation

of article 5.1.f) of the GDPR.

The claimant was at least able to access the data from the list he provided. the same listing

It appeared until 01/24/2022 in the browser, proving the aforementioned infraction.

IV.

Classification of the infringement of article 5.1.f) of the GDPR

Violation of article 5.1.f) of the GDPR supposes the commission of the typified infraction

in article 83.5 of the GDPR that under the heading "General conditions for the

imposition of administrative fines" provides:

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

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

overall annual total business of the previous financial year, opting for the one with the highest

amount:

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

consent under articles 5, 6, 7 and 9; (…)"

In this regard, the LOPDGDD, in its article 71 "Infractions", establishes that

"Infractions are the acts and conducts referred to in sections 4, 5 and

6 of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to the

present organic law".

For the purposes of the limitation period, article 72 "Infractions considered very serious"

of the LOPDGDD indicates:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679,

are 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 in violation of the established principles and guarantees

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

V

Penalty for violation of article 5.1.f) of the GDPR

Article 83 "General conditions for the imposition of administrative fines" of the

GDPR section 7 establishes:

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

58, paragraph 2, each Member State may establish rules on whether it can, and in

what measure, to impose administrative fines on state public authorities and bodies

established in that Member State."

Likewise, article 77 "Regime applicable to certain categories of responsible

or managers of the treatment" of the LOPDGDD provides the following:

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

who are responsible or in charge:...

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

autonomous entities and the entities that make up the Local Administration…

2. When the managers or managers listed in section 1 commit

any of the offenses referred to in articles 72 to 74 of this organic law,

the competent data protection authority will issue a resolution

sanctioning them with warning. The resolution will also establish the

measures that should be adopted to cease the conduct or to correct the effects of the

offense that was committed.

(…)

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 to the

under this article. (…)"

Therefore, the aforementioned infringement of article 5.1.f) of the GDPR, would be punishable with notice to the claimant.

SAW

GDPR Article 32

Article 32 of the GDPR establishes:

“Safety of treatment

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

a) the pseudonymization and encryption of personal data;

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

c) the ability to restore the availability and access to personal data in a manner fast in case of physical or technical incident;

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

2. When evaluating the adequacy of the level of security, particular account shall be taken of the risks presented by the data processing, in particular as a consequence of the destruction, loss or accidental or unlawful alteration of personal data transmitted, stored or otherwise processed, or unauthorized communication or access to

said data.

3. Adherence to an approved code of conduct pursuant to 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 controller and the processor shall take measures to ensure 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 such data following instructions from the responsible, unless it is obliged to do so by Union law or the Member states".

Recital 75 of the GDPR lists a series of factors or assumptions associated with risks to the guarantees of the rights and freedoms of the interested parties: "The risks for the rights and freedoms of natural persons, seriousness and probability variables, may be due to data processing that could cause damage and physical, material or immaterial damage, particularly in cases in which the treatment may give rise to problems of discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorized reversal of pseudonymization or

any other significant economic or social damage; in cases where it is deprived interested parties of their rights and freedoms or are prevented from exercising control over their personal information; in cases in which the personal data processed reveal the origin

ethnic or racial, political opinions, religious or philosophical beliefs, militancy in unions and the processing of genetic data, data relating to health or data on the sex life, or criminal convictions and offenses or related security measures; in cases in which personal aspects are evaluated, in particular the analysis or prediction of aspects related to work performance, economic situation, health, preferences or personal interests, reliability or behavior, situation or movements, in order to create or use personal profiles; in cases where process personal data of vulnerable people, in particular children; or in cases where for which the processing involves a large amount of personal data and affects a large number of interested parties.

Each treatment must be subject to a set of security measures according to the probability and risk to the rights and freedoms of natural persons, which must be be determined with reference to the nature of what the cancer was like as the context and purposes of data processing and such risk must be weighed on the basis of a objective assessment

Recital 83 states that "in order to maintain security and prevent the treatment infringes the provisions of this Regulation, the person in charge or the person in charge must assess the risks inherent to the treatment and apply measures to mitigate them" "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 with respect to the risks and the nature of the data personnel that must be protected. When assessing the risk in relation to the data security, the risks arising from of the processing of personal data, such as destruction, loss or accidental or unlawful alteration of personal data transmitted, stored or otherwise processed, or unauthorized communication or access to such

data, susceptible in particular to cause physical damages,

material or immaterial". The risk is thus related to the measures that have been

to be taken, which also have to be adequate

Those that are cited in article 32 of the GDPR, are a non-exhaustive set of those that are

they can take

In this case, what was intended to be published was a plenary call, which in

At first it would deal with the agenda items for discussion. In its place was introduced

another file and in another format from which the three infringing conducts arise.

It is based on the publication of the file at the headquarters, so that the public could access it, and

download the file taking into account the type of content, the format and the

preview before its effective publication, given the risks that said

type of treatment that prevents or helps to prevent the risks from occurring.

The claimant must have a solid and complete protocol that must not only prevent

that the contingency occurs, but, once it has occurred, in your case, as

corrective, react to the materialization of risk, which when applied, may

guarantee security in the processing of information and data.

The taking of measures must include the impact on the rights and freedoms

could have an incident, it occurs accidentally, man-made, natural or

technology and aim both to reduce the impact and its probability, which must be

be in constant renewal and improvement

In this case, when the initial correction (...) was produced, it was not taken into account that the

document, due to the form and means of implementation, remained in effect as a manager of contents, being able to be viewed in the browser, without technically having taken into account the operation of the application that generates the content, nor having counted on the participation in the process of specialized technical personnel such as computer science that seems obvious, if you know the effects of publication in electronic headquarters and in browser.

Failures in security measures that employees may commit in a legal entity, will not be charged to it as long as it has adopted all the measures of possible prevention, and in this case, it is considered that this verification as a measure technique, in relation to the nature of the treatment, the technology used: exposure in electronic headquarters with a content manager computer program in addition to need a prompt response in case of bankruptcy, requires these elements as reasonably demandable, elements that did not take place at the time. by not tackling completely the gap produced, because they were not established when the incidents. The defendant must have correctly assessed the risks of the lack of confidentiality in their additional risk identification protocols generated by the gap including those corresponding to human actions. Besides, the technology adopted in the treatment of publication with a tool of management of content that as a support was not present in the aforementioned protocol, having to add it when it was discovered that the failure was obeyed. Therefore, the lack of a correct consideration of attention to the organizational and technical measures in the configuration of the security measures violated in this case.

- To this must be added that the claim is transferred to the claimant on ***DATE.2, received on 05/04/2021, letting him know the facts, without obtaining a response, leaving time elapses without responding to the request. The AEPD already addressed the defendant in writing in phase of previous actions on 09/10/2021 in electronic notification modality and

having to reiterate by post, when rejecting the first, receiving the latter the

*** DATE.4 without obtaining attention to what was requested, to finally receive it on 01/25/2022

the defendant's brief, in which, among other things, he explains that "the delay in the

response was due to the fact that in said period there was a transition of responsibilities in

matters of data protection between the Information Security Committee, body

consultative and strategic for decision-making in matters of Security of the

Information, and the Data Protection Officer whose inauguration took place on

10/1/2021."

- When a letter of 01/25/2022 is received from the defendant, the first thing it indicates is that

responds to the request for information sent, received on ***DATE.4, and it was not known

even the survival of the information in the browser, which was completed on 12/1/2021.

In the request for information, the URL is made known to the electronic office as well as

as the https address.

In addition, up to twelve information questions were requested, which were answered

sequentially, and in the actions taken, the correction of 01/24/2022 is not alluded to

expressly, In the answer given in point 9 about the security violation and

Notification does not indicate any aspect either, extending the takeover of the DPD

related to the lack of notification to the control authority

Regarding the clarification of the correction of the survival of the possibility of access,

it was only indicated that "As of today 01/24/2021, the IT Department

has proceeded to review all the information content stored and published both in the

web as in the municipal headquarters, not having found any resource in support

similar or in whose content there is personal data".

The withdrawal of the URL from the content manager is fully known in the period of

tests when expressly requested in one of them and is answered specifying

that has been removed from the content manager with the intervention of the unit of

computing on 01/24/2022.

It was also clarified the purpose and object of the list of data that before said

test was not explained.

Thus, it is not true that the details of the infringement were known when it was

agreed to start the procedure.

In addition, whether or not the claimant is interested in the procedure, whether their data is

affected or not, does not affect the validity of said agreement, since the procedure is

always starts ex officio. (art 58 of the LPCAP). Nor the manifestation that there is no

evidence on the actual impact on rights would imply that the supervisory authority can

request and verify compliance with the obligations imposed by the GDPR, obtain

an explanation of what happened, and analyze the existing and derived measures. He

The fact that a real condition is not accredited to third parties does not mean that there is not

there was or could have been, certifying that the data have become evident

risk when several months elapse with the possibility that the browser obtained

the results, either by directly accessing its literal, or by other means.

It is proven that the defendant has infringed the aforementioned article.

VII

Classification of the infringement of article 32 of the GDPR

If confirmed, the aforementioned infringement of article 32 of the GDPR could entail the commission of the offenses typified in article 83.4 of the GDPR that under the rubric "General conditions for the imposition of administrative fines" provides:

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 of a company, in an amount equivalent to a maximum of 2% of the volume of overall annual total business of the previous financial year, opting for the one with the highest amount:

a) the obligations of the controller and the person in charge under articles 8, 11, 25 to 39, 42 and 43; (…)"

For the purposes of the limitation period, article 73 "Infringements considered serious" of the LOPDGDD indicates:

"Based on what is established in 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:

(…)

"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.

(…)

VIII

Penalty for violation of article 32 of the GDPR

In accordance with the application of articles 83.7 of the GDPR and 77.1.c) of the

LPDGDD, as explained in the legal basis V for the violation of article

5.1.f) of the GDPR, it would be appropriate to penalize the person claimed by the

infringement of article 32 of the GDPR.

IX

GDPR Article 33

Article 33 "Notification of a violation of the security of personal data to the

control authority" of the GDPR, establishes:

"1. In the event of a breach of the security of personal data, the person responsible for the

treatment will notify the competent control authority in accordance with the

article 55 without undue delay and, if possible, no later than 72 hours after

was aware of it, unless it is unlikely that said violation of the

security constitutes a risk to the rights and freedoms of natural persons.

If the notification to the control authority does not take place within 72 hours, it must go

accompanied by an indication of the reasons for the delay.

…

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

a) describe the nature of the breach of personal data security,

including, where possible, the categories and approximate number of stakeholders

affected, and the categories and approximate number of personal data records

affected;

b) communicate the name and contact details of the data protection officer or

another point of contact where more information can be obtained;

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

personal;

d) describe the measures adopted or proposed by the data controller to

remedy the breach of personal data security, including, if

appropriate, the measures adopted to mitigate the possible negative effects.

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

it is, the information will be provided gradually without undue delay.

5. The data controller shall document any breach of the security of the data

personal data, including the facts related to it, its effects and the measures

corrective measures adopted. Said documentation will allow the control authority to verify

compliance with the provisions of this article."

In the present case, it is clear that the defendant has suffered a security breach of the

personal data as of 03/31/2021 and you have not informed this Agency.

A data breach can have a number of adverse effects

considerable damage to people, capable of causing physical damage,

material or immaterial. The GDPR explains that these effects may include the

loss of control over your personal data, the restriction of your rights, the

discrimination, identity theft or fraud, financial loss, reversal

unauthorized pseudonymization, damage to reputation and loss of

confidentiality of personal data subject to professional secrecy. Also can

include any other significant economic or social harm to those persons.

In accordance with the principle of proactive responsibility, it would not be mandatory to notify all

breaches, since the controller could guarantee that the data breach is unlikely to

personal data involves a risk to the rights and freedoms of individuals

physical.

The defendant has defined the relationship that the collective owner of the data has with the City Council, which was to facilitate the modification of driving licenses and circulation of vehicles due to change of address that could be carried out more comfortably in the City Hall office. However, faced with this facilitation of

procedures, from (...) to 01/24/2022, there has been a possible and certain risk that in internet, not at the headquarters, it was possible to access a series of data that make up the identity of people with the simultaneous gathering of various data that add information about them, which is likely to constitute a risk to the rights and freedoms of those people.

When a personal data breach occurs, it is necessary for the person responsible determine rigorously what the possible consequences are, how they can affect the rights and freedoms of the people affected, that is, the level of severity with which such consequences could materialize and the likelihood of that they materialize The allegation made to avoid having to notify the gap that the "Information that could have been accessed by third parties could cause damage to those affected, but initially no serious damage is observed" does not serve as an excuse so that considering certainly that regardless of knowing how many people have been able to access it during the time the information was exposed, yes that points to the certain existence of risks to the rights and freedoms of seventeen affected by the infringement, given the joint content of the various data that are made known, and their relevance in affecting rights and freedoms, that with

regardless of whether damages have occurred to those affected, which is not

refers to the type, the authority is obliged to be notified.

The facts are considered to violate article 33 of the GDPR.

x

Classification of the infringement of article 33 of the GDPR

The infringement of article 33 of the GDPR supposes the commission of an infringement classified in

Article 83.4 of the GDPR which provides:

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

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

overall annual total business of the previous financial year, opting for the one with the highest

amount:

a) the obligations of the controller and the person in charge under articles 8, 11, 25 to

39, 42 and 43; (…)”

In this regard, the LOPDGDD, in its article 71, indicates: "Infractions" establishes that

"Infractions are the acts and conducts referred to in sections 4, 5 and

6 of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to the

present organic law”.

For the purposes of the limitation period, article 73 "Infringements considered serious" of

the LOPDGDD, indicates:

"Based on what is established in 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:

(…)

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

a breach of security of personal data in accordance with the provisions of the

Article 33 of Regulation (EU) 2016/679. (…)”

eleventh

Penalty for violation of article 33 of the GDPR

In accordance with the application of articles 83.7 of the GDPR and 77.1.c) of the

LPDGDD, as explained in the legal basis V for the violation of article

5.1.f) of the GDPR, it would be appropriate to penalize the person claimed by the

infringement of article 33 of the GDPR.

Therefore, in accordance with the applicable legislation and assessed the criteria of

graduation of sanctions whose existence has been accredited,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: SANCTION THE CITY COUNCIL OF GETAFE, with NIF P2806500A,

with a warning for each of the following infractions:

-Of article 5.1.f) of the GDPR, in accordance with article 83.5.a) of the GDPR, and

effects of prescription, classified as very serious, according to article 72.1 a) of the

LOPDGDD.

-Of article 32 of the GDPR, in accordance with article 83.4.a) of the GDPR, and

effects of prescription, classified as serious, according to article 73. f) of the

LOPDGDD.

- Article 33 of the GDPR, in accordance with article 83.4.a) of the GDPR, and

effects of prescription, classified as serious in article 73.r) of the LOPDGDD

SECOND: NOTIFY this resolution to GETAFE CITY COUNCIL.

THIRD: COMMUNICATE this resolution to the Ombudsman, in

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

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

This Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process 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 reversal before the

Director of the Spanish Agency for Data Protection within a period of one month from

count 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 07/13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided for in article 46.1 of the

referred Law.

Finally, it is noted 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 to the Spanish Data Protection Agency,

presenting it to

the agency

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

remaining records provided for in art. 16.4 of the aforementioned Law 39/2015, of 1/10.

You must also transfer to the Agency the documentation proving the

effective filing of the contentious-administrative appeal. If the Agency did not have

knowledge of the filing of the contentious-administrative appeal within the term

of two months from the day following the notification of this resolution, would give

by the end of the precautionary suspension.

Electronic record of

through the

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-181022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es