 File No.: EXP202102056

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claiming party) dated July 27, 2021

filed a claim with the Spanish Data Protection Agency. The

claim is directed against the ISLAND COUNCIL OF EL HIERRO with NIF

P3800003J (hereinafter, the claimed party / the CABILDO). The reasons on which it is based

the claim are as follows:

The web address in question is:

***URL.1

The document is a record of a plenary session of the Island Council of El Hierro in 2007, in the

that the matter "REPORT - PROPOSAL FOR A RESOLUTION OF THE TOWN

ISLAND OF EL HIERRO IN THE SEGREGATION RECORD OF EL PINAR".

The document contains an annex with the title: "ALLEGATIONS FILE OF

SEGREGACIÓN DE EL PINAR", which includes numerous personal data.

SECOND: In order to verify the existence of the denounced facts, in

September 2021, a Google search is carried out for the name and surname of the

claimant, the first result that appears indexed in the search engine is "REPORT -

PROPOSED RESOLUTION OF THE ISLAND COUNCIL OF EL HIERRO IN THE

SEGREGATION FILE OF EL PINAR"; the screenshot of the search

carried out is incorporated into the file.

By accessing the link of that first result, you can access the minutes of a plenary session

extraordinary session of the Island Council of El Hierro in 2007, in which the matter was discussed

"REPORT - PROPOSED RESOLUTION OF THE ISLAND COUNCIL OF EL

IRON IN THE SEGREGATION FILE OF EL PINAR". The document

contains an annex with the title: "ALLEGATIONS FILE OF

SEGREGACIÓN DE EL PINAR", which includes numerous personal data.

The record is incorporated into the file.

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

December, Protection of Personal Data and guarantee of digital rights (in

hereinafter LOPDGDD), said claim was transferred to the claimed party, the

TOWN HALL, to proceed with its analysis and inform this Agency within the term

of one month, of the actions carried out to adapt to the foreseen requirements

in the data protection regulations.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP), was collected on 09/23/2021 as stated in the

acknowledgment of receipt in the file.

On 09/23/2021, the Data Protection Delegate of the CABILDO presents

letter addressed to the AEPD in which he communicates that he has received the following email from the

AEPD: "On 09/17/2021, to the data controller "CABILDO DE EL

IRON" has been sent a notification from the AEPD by NOTIFIC@, which

informs you in his capacity as Delegate of Data Protection of

this entity" and asks how can you find out which person in charge has received the

notification or what notification does it refer to? Because none is indicated in the email

Additional Information.

In this regard, it should be noted, first of all, that the notice to the email address

email informing you of the availability of a notification at the headquarters

email address of the corresponding Administration or at the email address

single authorized authorization is an obligation of the Public Administrations, in accordance with the

established in article 41.6. of Law 39/2015, of October 1, on Procedure

Common Administrative Law, which establishes that: “6. Regardless of whether the

notification is made on paper or by electronic means, the Administrations

Public will send a notice to the electronic device and/or to the email address

email address of the interested party that the interested party has communicated, informing him of the

provision of a notification in the electronic headquarters of the Administration or

Corresponding body or at the unique authorized electronic address. the lack of

practice of this notice shall not prevent the notice from being fully considered

valid”.

And secondly, it should be noted that the notification was sent to the CABILDO DE EL

HIERRO and referred to the request for information on the claim filed

by the complaining party.

In response to the aforementioned letter dated 10/29/2021, it is sent to the DPD of the CABILDO

letter of "Request for additional documentation", which was collected on date

11/02/2021 as stated in the acknowledgment of receipt in the file.

Without the date of admission for processing of the claim presented

received a response neither to the letter of transfer nor to the request for additional information.

FOURTH: On December 23, 2021, in accordance with article 65 of the

LOPDGDD, the claim presented by the claimant party was admitted for processing.

FIFTH: On 03/02/2022, a Google search was carried out for the name and

surname of the claimant, the "REPORT -

PROPOSED RESOLUTION OF THE ISLAND COUNCIL OF EL HIERRO IN THE

FILE OF SEGREGATION OF EL PINAR".

Likewise, it is verified that when trying to access the URL in which supposedly

contained the data object of the formulated claim,: ***URL.1, gives an error,

indicating the non-availability of the information contained in the web page with which

it is no longer possible to access the document containing the minutes of the extraordinary plenary session of the

Island Council of El Hierro in 2007, in which the matter "REPORT -

PROPOSED RESOLUTION OF THE ISLAND COUNCIL OF EL HIERRO IN THE

FILE OF SEGREGATION OF EL PINAR"

These screenshots are incorporated into the file by diligence.

SIXTH: On March 17, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate disciplinary proceedings against the claimed party,

for alleged violations of Article 5.1.f) of the GDPR, classified in Article 83.5

of the GDPR and Article 32 of the GDPR, typified in Article 83.4 of the GDPR.

SEVENTH: On July 4, 2022, a resolution proposal was formulated,

proposing that the Director of the Spanish Data Protection Agency

penalize with three warnings for each of the offenses charged to the

COUNCIL OF EL HIERRO with NIF P3800003J:

- Warning for an infringement of Article 5.1.f) of the GDPR, typified in the

- Warning, for a violation of Article 30 of the GDPR, typified in the

- Warning, for a violation of Article 32 of the GDPR, typified in the

Article 83.5 of the GDPR.

Article 83.4 of the GDPR.

Article 83.4 of the GDPR.

And, likewise, it was proposed that the Director of the Spanish Agency for the Protection of

Data is imposed on the ISLAND COUNCIL OF EL HIERRO, with NIF P3800003J, the

adoption of measures to adapt their personal data processing to

the requirements of the data protection regulations, specifically, the performance of

Risk Analysis, of the adoption of security measures derived from the

themselves, the preparation of a register of treatment activities and the publication

of the inventory of the Registry of processing activities for which the

CABILDO, as well as the contribution of accrediting means of compliance with the

required, by virtue of the provisions of article 58.2 of the GDPR.

In issuing said resolution proposal, it was taken into account that once the agreement was notified

from the start, on 04/25/2022, the defendant filed a brief in which, in summary,

stated that it acknowledged receipt of the letter sent by the Spanish Agency of

Data Protection, in relation to the initiation of disciplinary proceedings for

claim formulated by Mr. A.A.A., No. XXXXXXXXX (writing of transfer of the

claim), for which it is requested that the information indicated be analyzed and sent

next:

“Regarding point 1.- Detailed description of the facts:

The CABILDO certifies that on October 18, 2006, the procedures

necessary in the different administrations for the initiation of segregation and

constitution of the new municipality of El Pinar, on the Island of El Hierro, in accordance with the Royal

Decree 1690/1986, of July 11, which approves the Population Regulations

and Territorial Demarcation of Local Entities.

After overcoming the different processes and requirements of various kinds (administrative,

economic, popular...), on April 17, 2007, the Plenary approved

Extraordinary session of the Island Council the proposal for segregation and constitution

from the municipality of El Pinar; publishing the Minutes of said plenary session in the

transparency portal (at that time general portal) of the Cabildo de El Hierro.

Regarding points 2 to 5.- Regarding the causes of the incident and the information

about those affected:

The TOWN HALL recalls that at that time there were no regulations of a

insular or autonomous community with respect to this matter, for which reason the Law

15/1999, of December 13, regarding the protection of personal data.

That no information related to ideology, religion or

beliefs of the affected.

Likewise, the COUNCIL indicates that the communication of data between

administrations and a third party did not need the consent of the affected party since

these data were intended to be processed for statistical purposes for a question

of public interest, in accordance with article 11 section E) of the aforementioned standard. And it is that

this hearing process was necessary in accordance with article 84 of the already repealed Law

30/1992, on the Legal Regime of Public Administrations and Procedure

Common Administrative Law, which establishes that "before the drafting of the proposal for

resolution, a hearing process must be given to the interested parties so that they could

reveal the allegations, information and data necessary or related to

The file."

The Cabildo also indicates that the gap between the information published in 2007

and the regulatory requirements subsequently required affects 3,996 people

residents in the segregated municipality and extra-municipal interested parties, whose data

published are of a personal nature, for which those affected can see

affected their right to intimacy, privacy or inviolability of the home, among

others.

And that the gap has been caused not by malpractice or error in copyright law

our corporation, if not for the absence (justified, since there was no imperative norm

to regulate this function) at that time of a system of transparency and

protection of personal data as effective and rigorous as that which exists in the

present.

With regard to points 7 and 8.- Regarding the request for remittance of the

data security measures and the Copy of the Activity Record of the

treatments:

The CABILDO maintains that the requirement of transparency and data protection is not

consolidated as an obligation of the administration until well after the date of

incident, so we do not have reports on the security measures of the

treatments, the supporting documentation of the Risk Analysis or the Registry

of Activity of the treatments where the incident occurred. It is not until 2019, in

accordance with the obligations imposed in the Organic Law 3/2018, of 5

December, Protection of Personal Data and guarantee of digital rights,

when a specific area is created for the correct treatment and defense of the

personal rights and administrative transparency required of this corporation.

9 and 10.- Finally, regarding the notification to those affected and to the Spanish Agency for

Data Protection of this incident we emphasize that:

This controversy assumes relevance 14 years later due to the absence in that

then of insular, regional, national or European regulations on the protection of

personal data that we are aware of today, but that at no time

was carried out with intent to undermine or for purposes detrimental to the

interested. On the contrary, from this corporation it was necessary to publish

said data for the joint implementation of public opinion and consensus and causes

of this, among the population, in order to carry out a transformation of this

size at island level. Due to the long period elapsed and the different evolution

regulations on the matter adopted in the last 14 years, this security breach

It has not been revealed or communicated (since it is unknown) until

the day of receipt of this notification.

6 and 11.- Therefore, to correct and preserve the right to privacy and protection of

data of those affected, the Cabildo de El Hierro has proceeded to eliminate the

Minutes published and their rectification, which will not include any data whose

public exposure may compromise the rights of those affected.

In addition, an attempt will be made to review the documents published by this Corporation that

include data of this nature, and proceed to correct them in the indicated sense".

These statements were duly answered in the proposed resolution.

EIGHTH: Notification of the aforementioned resolution proposal in accordance with the rules

established in Law 39/2015, of October 1, on Administrative Procedure

Common for Public Administrations (hereinafter, LPACAP) and after the

period granted for the formulation of allegations, it has been verified that there has been no

received any allegation by the claimed party.

PROVEN FACTS

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

6/19

FIRST: A.A.A. (hereinafter, the claiming party) dated July 27, 2021

filed a claim with the Spanish Data Protection Agency. The

claim is directed against the ISLAND COUNCIL OF EL HIERRO with NIF

P3800003J (hereinafter, the claimed party / the CABILDO). The reasons on which it is based

the claim are as follows:

The web address in question is:

***URL.1

The document is a record of a plenary session of the Island Council of El Hierro in 2007, in the

that the matter "REPORT - PROPOSAL FOR A RESOLUTION OF THE TOWN

ISLAND OF EL HIERRO IN THE SEGREGATION RECORD OF EL PINAR".

The document contains an annex with the title: "ALLEGATIONS FILE OF

SEGREGACIÓN DE EL PINAR", which includes numerous personal data.

SECOND: In September 2021, a Google search is performed for the

name and surname of the claimant, the first result that appears indexed in the

search engine is "REPORT - RESOLUTION PROPOSAL OF THE ISLAND COUNCIL

OF EL HIERRO IN THE RECORD OF SEGREGATION OF EL PINAR"; the

Screenshot of the search performed is incorporated into the file.

By accessing the link of that first result, you can access the minutes of a plenary session

extraordinary session of the Island Council of El Hierro in 2007, in which the matter was discussed

"REPORT - PROPOSED RESOLUTION OF THE ISLAND COUNCIL OF EL

IRON IN THE SEGREGATION FILE OF EL PINAR". The document

contains an annex with the title: "ALLEGATIONS FILE OF

SEGREGACIÓN DE EL PINAR", which includes numerous personal data.

The record is incorporated into the file.

THIRD: On 03/02/2022, a Google search was carried out for the name and

surname of the claimant, the "REPORT -

PROPOSED RESOLUTION OF THE ISLAND COUNCIL OF EL HIERRO IN THE

FILE OF SEGREGATION OF EL PINAR".

Likewise, it is verified that when trying to access the URL in which supposedly

contained the data object of the formulated claim,: ***URL.1, gives an error,

indicating the non-availability of the information contained in the web page with which

it is no longer possible to access the document containing the minutes of the extraordinary plenary session of the

Island Council of El Hierro in 2007, in which the matter "REPORT -

PROPOSED RESOLUTION OF THE ISLAND COUNCIL OF EL HIERRO IN THE

FILE OF SEGREGATION OF EL PINAR"

FOURTH: The COUNCIL in its letter dated 04/25/2022 states that it does not count

with reports on the security measures of the treatments, of the

Documentation accrediting the Risk Analysis or the Register of Activity of the

treatments where the incident occurred.

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 and 48.1 of the Law

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

digital rights (hereinafter, LOPDGDD), is competent to initiate and resolve

this procedure the Director of the Spanish Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that: "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

On 04/25/2022, the defendant filed a brief in relation to the "Agreement to initiate

disciplinary procedure: Claim against the Cabildo de El Hierro for

violation of personal data" that contains the response to the transfer of the

claim presented by the claimant, and whose content will be treated as

allegations to the initiation agreement.

In response to the allegations presented by the respondent entity, it should be noted

the next:

In relation to point 1.- Detailed description of the facts from which the

the claim; these are none other than the segregation and constitution of the new

municipality of El Espina on the Island of El Hierro, whose procedures begin on 10/18/2006 and

end with their approval by the Extraordinary Plenary of the Island Council of 04/17/2007

and its publication on the transparency portal of the Cabildo. To this description that

carried out by the CABILDO, it is only necessary to add that the publication of the Minutes of the Plenary and of the Annexes containing the personal data that have given rise to the processing of this sanctioning procedure was kept on the transparency portal from 2007 to 2021.

It should be noted that the purpose of the transparency portal is to promote the transparency of public activity, ensure compliance with the obligations of publicity, safeguard the exercise of the right of access to public information and ensure compliance with good governance provisions; fulfilled these purposes, action should have been taken on the personal data published for the purpose to minimize them and that they only remain accessible for the time necessary to the purposes of the treatment, as required in article 5 paragraphs c) ["principle of

minimization of data] and e) [principle of limitation of the conservation period] of the GDPR.

Corresponding to the COUNCIL, as responsible, adapt the treatment that supposes the publication of their acts in their transparency profile, to the new regulations of Data Protection.

Regarding points 2 to 5.- Regarding the causes of the incident and the information about those affected:

The TOWN HALL recalls that at that time there were no regulations of a insular or autonomous community with respect to this matter, for which reason the Law 15/1999, of December 13, regarding the protection of personal data.

That no information related to ideology, religion or

beliefs of the affected.

And that the communication of data between administrations and to a third party does not

It needed the consent of the affected party since these data were intended for the

processing for statistical purposes for a matter of public interest, in accordance with

article 11 section E) of the aforementioned standard. And it is that this hearing procedure was

necessary according to article 84 of the already repealed Law 30/1992, of Legal Regime

Public Administrations and Common Administrative Procedure, which

establishes that "before the drafting of the proposed resolution, the

hearing procedure for the interested parties so that they could reveal the

allegations, information and data necessary or related to the file."

The Cabildo also indicates that the gap between the information published in 2007 and

the regulatory requirements subsequently required affects 3996 people

residents in the segregated municipality and extra-municipal interested parties, whose data

published are of a personal nature, for which those affected can see

affected their right to intimacy, privacy or inviolability of the home, among

others.

And that the gap has been caused not by malpractice or error in copyright law

our corporation, if not for the absence (justified, since there was no imperative norm

to regulate this function) at that time of a system of transparency and

protection of personal data as effective and rigorous as that which exists in the

present.

Regarding the fact that at that time there were no regulations of an insular or

regarding this matter, for which Law 15/1999, of

December 13, since the gap between the information published and the requirements

regulations required later; It should be noted that Recital 171 of the

GDPR establishes the obligation that "All treatment already started on the date of

application of this Regulation must comply with this Regulation in the

period of two years from the date of its entry into force.

Anticipating in article 99 of the GDPR that “1. This Regulation shall enter into

force twenty days after its publication in the Official Journal of the European Union. [He

GDPR was published in DOUE L119, of May 4, 2016].

2. It will be applicable from May 25, 2018.

This Regulation shall be binding in all its elements and directly

applicable in each Member State.

Bearing in mind that, as the Legal Office has repeatedly pointed out,

of the AEPD, in the different consultations submitted to its report (valid by all

Reports N/REF: 0004/2022; 0089/2020) "the paradigm shift that the

full application of Regulation (EU) 2016/679 of the European Parliament and the Council,

of April 27, 2016, regarding the protection of natural persons in what

regarding the processing of your personal data and the free movement of such data

(GDPR), as it is based on the principle of "accountability" or responsibility

proactive, as stated in the Statement of Reasons of the Organic Law

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

digital rights (LOPDGDD): "the greatest novelty presented by the Regulation (EU)

2016/679 is the evolution of a model based, fundamentally, on the control of the

compliance to another that rests on the principle of active responsibility, which

requires a prior assessment by the person in charge or by the person in charge of the treatment of the risk that could be generated by the processing of personal data in order to Based on said assessment, adopt the appropriate measures".

Consequently, by virtue of said principle, the data controller must apply appropriate technical and organizational measures in order to guarantee and be able demonstrate that the treatment is in accordance with the Regulation."

Provided in Recital 39 that: "(...) Personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are treated. This requires, in particular, ensuring that their use is limited to a strict minimum. conservation period. Personal data should only be processed if the purpose of the treatment could not reasonably be accomplished by other means. To ensure that personal data is not kept longer than necessary, the person responsible for the treatment must establish deadlines for its suppression or periodic review".

Therefore, the Cabildo had to adapt, in the mentioned period, the treatment that supposes the publication of their acts in their transparency profile, to the new regulations of data protection, providing a period for the deletion or periodic review of the published data.

With regard to points 7 and 8.- Regarding the request for remittance of the data security measures and the Copy of the Activity Record of the treatments:

The CABILDO maintains that the requirement of transparency and data protection is not consolidated as an obligation of the administration until well after the date of incident, so we do not have reports on the security measures of the treatments, the supporting documentation of the Risk Analysis or the Registry

of Activity of the treatments where the incident occurred. It is not until 2019, in

accordance with the obligations imposed in the Organic Law 3/2018, of 5

December, Protection of Personal Data and guarantee of digital rights,

when a specific area is created for the correct treatment and defense of the

personal rights and administrative transparency required of this corporation.

As previously indicated, "the paradigm shift brought about by the

full application of Regulation (EU) 2016/679 of the European Parliament and the Council,

of April 27, 2016, regarding the protection of natural persons in what

regarding the processing of your personal data and the free movement of such data

(GDPR), as it is based on the principle of "accountability" or responsibility

proactive, as stated in the Statement of Reasons of the Organic Law

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

digital rights (LOPDGDD): "the greatest novelty presented by the Regulation (EU)

2016/679 is the evolution of a model based, fundamentally, on the control of the

compliance to another that rests on the principle of active responsibility, which

requires a prior assessment by the person in charge or by the person in charge of the treatment of the

risk that could be generated by the processing of personal data in order to

Based on said assessment, adopt the appropriate measures".

Consequently, by virtue of said principle, the data controller must

apply appropriate technical and organizational measures in order to guarantee and be able

demonstrate that the treatment is in accordance with the Regulation."

Without being able to excuse themselves for not establishing such measures and for not counting on

reports on security measures for processing, documentation

accrediting the Risk Analysis or the Activity Record of the treatments

where the incident occurred in which the requirement of transparency and protection of

data was not consolidated as an obligation of the administration until well after the date

of the incident

9 and 10.- Finally, regarding the notification to those affected and to the Spanish Agency for

Data Protection of this incident we emphasize that:

The CABILDO alleges that this controversy assumes relevance 14 years later before the

Absence at that time of island, regional, national or European regulations

on the protection of personal data that we know today, but

that at no time was it carried out with intent to undermine or for personal purposes

judgments for the interested party. On the contrary, from this corporation it was necessary the

publication of said data for the joint implementation of public opinion and the

consensus and causes of this, among the population, in order to carry out a

transformation of this magnitude at island level. Due to the long period that has elapsed and

the different normative evolution in the matter adopted in the last 14 years, this

security breach has not been disclosed or reported (at

not know the same) until the day of receipt of this notification.

As has already been proven, in the response to the previous allegations, it is not

the fact of the need to publish these data is questioned, but rather the lack of

adaptation of the publication to the new requirements demanded by the regulations of

data protection, that as responsible should have carried out the

COUNCIL.

6 and 11.- Therefore, to correct and preserve the right to privacy and protection of

data of those affected, the Cabildo de El Hierro has proceeded to eliminate the

Minutes published and their rectification, which will not include any data whose

public exposure may compromise the rights of those affected.

In addition, an attempt will be made to review the documents published by this Corporation that

include data of this nature, and proceed to correct them in the sense indicated

Regarding the allegation referred to points 6 and 11, note that it is considered

positive adoption of the measures to eliminate the published Act and to its

rectification, which will not include any data whose public exposure may

compromise the rights of those affected.

Likewise, it is also considered positive that the documents are reviewed

published by this Corporation that include data of this nature, and proceed to

correction in the indicated sense.

Considering that these measures contribute to limiting or preventing the rights of

affected may be violated by the public exposure of their data.

Although it is considered necessary for the COUNCIL to adopt the appropriate decisions to

accredit the security measures, the Risk Analysis or the Registry of

Treatment activities for which it is responsible.

II

The denounced facts are specified in that through the transparency portal of the

CABILDO, allowed access to the data of the claimant and the rest of the

residents of El Pinar de El Hierro, who made allegations in the file of

segregation of El Pinar, contained in the minutes of the extraordinary plenary session of the Cabildo

Insular de El Hierro of 2007, in which the matter "REPORT - PROPOSAL

RESOLUTION OF THE ISLAND COUNCIL OF EL HIERRO IN THE FILE OF

SEGREGATION OF EL PINAR", violating the principle of confidentiality.

Said treatment could constitute a violation of article 5 of the GDPR,

Principles related to treatment, which establishes that:

"1. Personal data will be:

(…)

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

personal data, including protection against unauthorized or unlawful processing and

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

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

(…)”

The documentation in the file offers clear indications that the party

claimed violated article 5.1.f) of the GDPR, principles relating to treatment, to

allow third parties, through the page of the transparency portal of the CABILDO, the

access to personal data of the residents who presented allegations in the

segregation procedure of El Pinar de El Hierro, and this despite the time

elapsed from the processing of the aforementioned procedure to the presentation of the

claim, more than fourteen years, without there being any evidence that

Appropriate security measures have been adopted to prevent access by third parties to such

data.

IV.

Article 30 of the GDPR establishes the obligation for those responsible to wear "a

record of the treatment activities carried out under its responsibility".

Provided in recital 82 of the GDPR that "To demonstrate compliance

with this Regulation, the controller or processor must

keep records of the processing activities under its responsibility".

And establishing in article 31.2 of the LOPDGDD that "The subjects listed

in article 77.1 of this organic law they will make public an inventory of their activities

of treatment accessible by electronic means in which the information will be recorded

established in article 30 of Regulation (EU) 2016/679 and its legal basis".

As stated in the fourth proven fact of this resolution, the COUNCIL in its

letter of 04/25/2022 states that it does not have reports on the security measures

security of the treatments, of the supporting documentation of the Analysis of

Risks or the Activity Record of the treatments where the incident occurred.

Failure to have a record of processing activities for which it is responsible

supposes a violation of article 30 of the GDPR, and not having published the Inventory

of treatment activities supposes a violation of article 31.2 of the

LOPDGDD.

V

Article 32 of the GDPR, security of treatment, establishes the following:

1. Taking into account the state of the art, the application costs, and the

nature, scope, context and purposes of processing, 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 and

appropriate organizational measures to guarantee a level of security appropriate to the risk,

which may include, among others:

a) the 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 assessment of the effectiveness of technical and organizational measures to ensure the safety of the treatment.

2. When evaluating the adequacy of the level of security, particular attention should be paid to take into account the risks presented by data processing, in particular as consequence of the destruction, loss or accidental or illegal alteration of data personal information transmitted, preserved or processed in another way, or the communication or unauthorized access to said data (The underlining is from the AEPD).

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 to the rights and freedoms of natural persons, serious and variable probability, may be due to data processing that could cause physical, material or immaterial damages and losses, particularly in cases in which that the treatment may give rise to problems of discrimination, usurpation of identity or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorized reversal of the pseudonymization or any other significant economic or social harm; in the cases in which the interested parties are deprived of their rights and freedoms or are

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

personal treaties reveal ethnic or racial origin, political opinions, religion

or philosophical beliefs, union membership and genetic data processing,

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

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

personal aspects, in particular the analysis or prediction of aspects related to the

performance at work, economic situation, health, preferences or interests

personal, reliability or behavior, situation or movements, in order to create or

use personal profiles; in cases in which personal data of

vulnerable people, particularly children; or in cases where the treatment

involves a large amount of personal data and affects a large number of

interested."

The facts revealed imply the non-accreditation of technical measures and

appropriate organizational procedures, by disclosing information and data of a personal nature to

third parties, with the consequent lack of diligence by the person responsible; every time I don't know

has proven that the claimed party had adopted some measure to guarantee

the anonymization of the information containing personal data was

hosted on its transparency portal, in order to comply with the regulations in

data protection matter.

SAW

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

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

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

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

From the documentation in the file, there are clear indications that the

claimed has violated article 32 of the GDPR, as a breach of

security, by allowing any third party, including the claimant, access, through

of the transparency portal of the CABILDO, to the minutes of the extraordinary session, revealing

information and personal data of the people who had made

allegations.

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

security measures that are applicable according to the data that is the object

of treatment, but it 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 processing, probability risks

and seriousness for the rights and freedoms of the persons concerned.

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

particular account of the risks presented by data processing, such as

consequence of the destruction, loss or accidental or illegal alteration of data

personal information transmitted, preserved or processed in another way, or the communication or

unauthorized access to said data and that could cause damages

physical, material or immaterial.

In this sense, recital 83 of the GDPR states that:

"(83) In order to maintain security and prevent processing from infringing the provisions of

this Regulation, the controller or processor must assess the risks

inherent to the treatment and apply measures to mitigate them, such as encryption. Are

measures must ensure an adequate level of security, including the

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

regarding the risks and nature of the personal data to be

protect yourself. When assessing risk in relation to data security, considerations should be

take into account the risks arising from the processing of personal data,

such as the destruction, loss or accidental or unlawful alteration of personal data

transmitted, stored or processed in another way, or communication or access not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

Article 83.5 of the GDPR provides the following:

VII

"5. Violations of the following provisions will be penalized, in accordance with the

paragraph 2, with administrative fines of maximum EUR 20,000,000 or,

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

total annual global business volume of the previous financial year, opting for

the highest amount:

to)

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

sentiment in accordance with articles 5, 6, 7 and 9;”

For its part, Article 71 of the LOPDGDD, under the heading "Infractions" determines what

following: "Infractions are 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.”

Establishes article 72 of the LOPDGDD, under the heading of "Infractions considered

very serious” for prescription purposes, the following: “1. Depending on what you set

Article 83.5 of Regulation (EU) 2016/679 are considered very serious and

Offenses that involve a substantial breach of law shall prescribe after three years.

of the articles mentioned therein and, in particular, the following:

(…)

to)

The processing of personal data in violation of the principles and guarantees

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

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

cited GDPR in the following terms:

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

paragraph 2, with administrative fines of maximum EUR 10,000,000 or,

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

total annual global business volume of the previous financial year, opting for

the highest amount:

to)

the obligations of the controller and the person in charge under articles 8, 11,

25 to 39, 42 and 43.”

(…)

Establishes article 73 of the LOPDGDD, under the heading "Infractions considered

serious" for prescription purposes, the following:

"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.

(…)

n) Not having the record of processing activities established in article 30

of Regulation (EU) 2016/679

In the present case, the infringing circumstances provided for in article

83.5 and 83.4 of the GDPR and 72.1.a) and 73 sections f) and n) of the LOPDGDD, above

transcribed.

VIII

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

GDPR in its section 7 establishes:

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

Article 58(2), each Member State may lay down rules on whether

can, and to what extent, impose administrative fines on authorities and bodies

public establishments established in that Member State."

Likewise, article 77 "Regime applicable to certain categories of

responsible or in charge 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 / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

17/19

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 law

organic, the data protection authority that is competent will dictate

resolution sanctioning them with a warning. The resolution will establish

likewise, the measures that should be adopted to cease the conduct or to correct it.

the effects of the offense 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, if any.

(…)

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."

In the present case, taking into account that the person responsible is an entity that is part of the

Local Administration, CABILDO DE EL HIERRO is considered in accordance with Law,

impose a warning sanction for violation of article 5.1.f); another sanction

of warning for infringement of article 30 of the GDPR, and another sanction of

warning for infringement of article 32 of the GDPR to the claimed party.

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: IMPOSE THE ISLAND COUNCIL OF EL HIERRO, with NIF P3800003J,

by:

-

-

-

an infringement of Article 5.1.f) of the GDPR and Article 32 of the GDPR, typified in

Article 83.5 of the GDPR, a warning sanction.

an infringement of Article 30 of the GDPR, typified in Article 83.4 of the

GDPR, a warning sanction.

an infringement of Article 32 of the GDPR, typified in Article 83.4 of the

GDPR, a warning sanction.

SECOND: TO ORDER the ISLAND COUNCIL OF EL HIERRO, with NIF P3800003J,

the adoption of measures for the adequacy of their personal data processing

to the requirements of the data protection regulations, specifically, the performance of

Risk Analysis, of the adoption of security measures derived from

the same, the elaboration of a register of treatment activities and the

publication of the inventory of the Register of treatment activities of which

The TOWN HALL is responsible, as well as the contribution of means accrediting the

compliance with what is required, by virtue of what is established in article 58.2 of the

GDPR.

The adoption of these measures must be carried out within a period of 4 months from

from the day following the notification of this resolution.

Documentation accrediting compliance with the AEPD must be provided

these measures within 10 days of the end of the 4-month period

Granted for adoption by the COUNCIL OF EL HIERRO.

THIRD: NOTIFY this resolution to the ISLAND COUNCIL OF EL

IRON.

FOURTH: COMMUNICATE this resolution to the Ombudsman, in

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 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 July 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 through

writing addressed to the Spanish Data Protection Agency, presenting it through

of the Electronic Registry of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registries 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 proceedings within a period of two months from the day following the

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es