 Procedure No.: PS/00187/2020

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and with

based on the following

BACKGROUND

FIRST: On January 14, 2020, the Subdirectorate General for Nationality

and Civil Status (hereinafter, SGNEC) attached to the General Directorate of Registries and

of Notaries (currently the General Directorate of Legal Security and Public Faith, in

hereinafter, DGSJFP) currently organically and functionally dependent on the

General Secretariat for the Innovation and Quality of the Public Service of Justice (in

hereinafter, SGICSPJ) of the Ministry of Justice, notifies this Spanish Agency of

Data Protection (hereinafter, AEPD) a data security breach

(hereinafter, security breach) after having knowledge through a

email by a citizen of a notification of granting of the

Spanish nationality corresponding to another person (treatment related to the

application ***APPLICATION.1).

The SGNEC contacted by telephone the director of the Information Technology Division

Information and Communications of the Ministry of Justice (currently the Division of

Technologies and Digital Public Services, hereinafter, DTSPD) to know the

nature and scope of the problem and the number of potentially affected notifications.

Finally, having confirmed the security breach, the SGNEC states that it was decided to

stoppage of automated notifications until the cause and scope of the

incident and its resolution.

SECOND: On February 4, 2020, the director of the AEPD agrees

initiate investigative actions, for which the Subdirectorate General for Inspection

of Data proceeded to carry out preliminary investigation actions for the

clarification of the facts object of the notification, having knowledge of the

following ends:

BACKGROUND

Date of the events: ***DATE.1

Date of detection of the security breach: ***DATE.2

Security bankruptcy notification date: 01/14/2020

INVESTIGATED ENTITIES

General Directorate of Legal Security and Public Faith of the Ministry of Justice with

NIF S2813610I and DIR3 E00131304, and with address at Plaza de Jacinto Benavente 3,

28012 Madrid (organically and functionally attached to the SGICSPJ with NIF S2813610I and

DIR3 E05077001 as data controller).

RESULT OF THE INVESTIGATION ACTIONS

1. Regarding the facts:

 Around 2:30 p.m. on ***DATE.2, the SGNEC stated that it had

received telephone communication in relation to the receipt of an email

electronically by a citizen of a notification of granting of the

Spanish nationality by residence corresponding to another applicant. In that

moment, the SGNEC contacted the DTSPD by telephone to find out the

nature of the problem and the number of notifications potentially

affected by the security breach, and it was decided to stop the

automated notifications until the cause of the incident is known and resolved.

No copy of the citizen's email is provided.

□

□

□

The SGNEC informs that on January 13, 2020 it received from the DTSPD

base report of the security bankruptcy notification that was communicated

to the AEPD on January 14, 2020. From the aforementioned report, the SGNEC

states that the incident reaches 34 cases and subsequently incorporated

another 2 more, up to 36, of the 23,394 nationality resolutions resolved

until that moment. There is no record of the intervention of the Protection Delegate of

Data in accordance with article 39 of the RGPD.

The SGNEC declares to have attached said report to the AEPD in its notification

security bankruptcy, and points out the following:

“The problem had its origin in a modification in the generation process

of resolutions granting nationality by residence that had been

made in the application ***APPLICATION.1, for processing files of

nationality by residence, on ***DATE.1”.

The SGNEC informs that the detected failure originated when attaching the certificate

of birth of the nationality applicant to the resolution document of

grant of nationality. The high number of resolutions generated from

concurrently is the consequence of a reinforcement plan that punctually

implies a scenario of high request concurrency. Also, the SGNEC

adds that said reinforcement plan has involved the participation of a number

much higher number of processing personnel than initially planned in the design of the

app.

The SGNEC points out that the personal data affected in the data breach

security would correspond to the NIE (Foreigner Identification Number),

name, surnames, place and date of birth, address at the time of

submit the application, the nationality grant itself and a copy of the

birth certificate (in which date and place data appear again

of birth and names and surnames of the parents).

The SGNEC reports that it has registered two other incidents of

security of personal data, on dates 06/28/2019 and 10/31/2019,

also with incorrect notifications due to recipient error when communicating

nationality concessions, with 11 and 70 people affected respectively

and already solved. The SGNEC states that the incident that occurred on 06/28/2019

derived from the process of sending telematic notifications for an incident in

the application database, while that of 10/31/2019 consisted of

an incorrect management of exceptions in the case of saturation of different

systems with which the application interacts, including the signature holder of the

Ministry of Justice.

The Data Inspection records that, on 09/05/2018, the

AEPD issued a sanctioning procedure resolution, of reference

AP/00049/2018, in which the now

investigated to the General Directorate of Registries and Notaries

dependent on the Undersecretary of Justice (now DGSJFP, dependent on the

SGICSPJ). Specifically, in the aforementioned sanctioning file it was accredited

that “The Information Technology and Communications Division of the

Ministry of Justice informed that the service did not contemplate the concurrence and

he made a mistake when composing the birth certificate. The volume and page that

appear on the certificate are correct and correspond to the details of your

birth registration, but the content with the digitized image is the

of another request, that of marriage”. (the underlining is from the AEPD).

2. Regarding the measures prior to the security breach event:

□

The SGNEC is currently identified in the RAT (Registry of

treatment activities) of the Ministry of Justice as responsible for the

processing of data in the management of applications for Spanish nationality.

The SGNEC provides an internal working document to update the RAT in

that DTSPD is specified as co-controller now

Analyzed as of January 2020.

□

□

□

The SGNEC states that it has carried out an EIPD (impact assessment on data protection) in June 2019, which contains an analysis of risks associated with the data processing it manages.

The SGNEC has a report on actions derived from the EIPD in the management of applications for Spanish nationality, which aims to minimize the potential risks analyzed through the implementation of various corrective actions until they are reduced to residual risks that have resulted be high level.

The DTSPD, as co-controller of the treatment (according to the RAT provided and in force since January 2020), has a procedure on the quality of the software projects of the Ministry of Justice throughout throughout its life cycle, which serves as the basis for its construction and development in the defining the phases that govern the analysis and design of the solution, as well as the tests that must be carried out in the different environments (development, integration, quality and pre-production), until its final implementation in the production environment, and active monitoring after it is put into production.

3. Regarding the measures after the event of the security breach:

3.1. Of a corrective nature (reactive to correct the security breach):

□

The SGNEC states that, once the incident was known, on ***DATE.2 at 2:30 p.m., the signing and notification process was blocked automated of the concessions of Spanish nationality in the application involved (***APPLICATION.1).

□ On Tuesday, January 14, 2020, the security breach was notified to the AEPD.

□

The SGNEC states that on Wednesday, January 15, 2020 at 3:50 p.m.

hours, the Citizen Folder is removed from the notifications

electronic documents of the concessions of Spanish nationality issued with

erroneous content when referring to another nationality applicant.

The SGNEC provides evidence that on Thursday, January 16, 2020,

electronically signed 72 trades communicating the security breach

both to the addressees of the resolutions and to the people who

received wrongly, the acknowledgments of receipt were completed,

enveloping and delivery notes for mailing to interested parties.

The SGNEC states that on January 21, 2020 the exit was registered

from the General Registry of the Ministry of Justice the list of

administrative notifications together with the envelopes, acknowledgments of receipt and

delivery notes for processing communications to interested parties.

The SGNEC informs that the signature process will be enabled again on the 23rd

January 2020 at 3:40 p.m., but not the notification process

of the concessions of Spanish nationality that continued

blocked as of February 26, 2020.

The SGNEC states that as of Friday, January 24, 2020 at

9:00 a.m. notifications of granting of

nationality manually after verifying that the document

to notify is correct.

3.2. Of a preventive nature (proactive to prevent the bankruptcy of

security):

-
-
-

The DTSPD claims to have designed in the application ***APPLICATION.1

a more robust measure that checks the content of documents

granting of Spanish nationality prior to notification,

in such a way that no document can be notified

corresponding in contents with the processed file. The SGNEC

reports that a prior quality control protocol has been established (not

details it) to ensure that the document to be notified is correct,

making the notification manually and supervised.

The DTSPD states that the new version is in the testing phase

of the application that incorporates in the notification process the reading and

verification of the content of the document to be communicated

prior to notification. The SGNEC conveys that the new version of the

application is (as of February 26, 2020) undergoing controls

of quality (functional tests, performance tests and tests of

concurrence).

The DTSPD reports having detected the origin of the security breach

in an inappropriate handling of temporary files when performing the annexation of

the birth certificate to the decision granting nationality.

Additionally, the SGNEC highlights that work is being done on the

implementation of an automatic process that goes through the forms of the

application and that allows an additional quality control to be carried out

made in the application options, in such a way as to guarantee

that the resolutions granting Spanish nationality are

notified correctly.

 As of the date of this agreement, the Data Inspection of the AEPD

has not been informed of the progress and guarantees established/implemented

in the new app/version of grant notifications

nationality, as well as the tests in the new version of November

2019 carried out, risk analysis, impact assessment on

rights and freedoms of the data subjects and whether the incident has been resolved.

THIRD: On July 9, 2020, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimant, for the

alleged infringement of Article 32 of the RGPD, Article 5.1.f) of the RGPD, Article 25 of the

RGPD, typified in Article 83.5 of the RGPD.

FOURTH: On October 7, 2020, a resolution proposal was formulated,

proposing in the following terms:

<<That the Director of the Spanish Data Protection Agency sanction

the General Secretariat for the Innovation and Quality of the Public Service of Justice, with

NIF S2813610I, by:

1.

two.

3.

Infringement of article 5.1.f) of the RGPD typified in article 83.5.a) of the RGPD

with a penalty of warning.

Violation of articles 25, 32 and 33 of the RGPD in relation to the article

5.1.f) of the RGPD, typified in article 83.4.a) of the RGPD with sanction of

warning.

Infringement of article 34 of the RGPD in relation to article 5.1.f) of the RGPD,

typified in article 83.4.a) of the RGPD, with a penalty of warning.

4. And require the SGICSPJ to provide this AEPD with a summary of the final result

of the action plan, already started in February 2020, which applies

more robust security measures in data processing in the

application ***APPLICATION.1 for which it is responsible in terms of protection

of data through the SGNEC>>.

FIFTH: On 10/23/2020, the respondent presents allegations to the proposal of

resolution in the following terms:

In the first place, the respondent considers that there was no breach of integrity, since

which, as defined by the National Security Scheme (ENS), integrity is

that “property or characteristic that the information asset has not

been altered in an unauthorized manner”, so it is not applicable to this

case.

In this regard, it should be noted that the new principle of integrity, previously called

security, collected in article 5.1. f) of the RGPD, brings cause of the provisions of the

Article 1 of the aforementioned regulation (object of the RGPD) regarding the processing of data

personal in a broad sense and with temporal projection regardless of the

specific data that are subject to treatment, and not only with respect to specific data

and static over time for a given treatment. Consequently, the

claim must be rejected.

Secondly, regarding the dimension of confidentiality of the data processed, the

investigated indicates that it was limited to 36 direct people and another 36 indirectly,

so it was produced to a finite and determined number of persons, and not to a

number of indeterminate persons, as indicated in article 25.2 of the RGPD.

In this sense, it means that the indeterminacy referred to in the article

25.2 of the RGPD refers to the principle of design by default under which the

technical and organizational measures applied shall in particular ensure that, by default,

personal data is not accessible to an indeterminate number of people

physical, and not the number of people affected by the breach. Consequently, the

claim must be rejected.

Thirdly, it provides a set of measures taken that are reactive and

proactive, from which a diligent conduct emerges in order to minimize the

impact of the breach and prevent similar situations from recurring in the future. In this

sense provides a documentary on new quality actions in the code, tests

functions that especially contemplate the concurrence of requests and composition

of documents to be notified, review of the life cycle, training of the

development and regular monitoring plan of the code quality plan.

Fourth, the respondent provides a documentary on the bidding for a file
of hiring for the adequacy of the treatments carried out in the unit to the
ENS, starting its execution in September 2020, reinforcing the policies of
security by both the personnel assigned to the DTSPD and its main
service providers acting as data processors. To this end,
provides specifications of technical prescriptions that govern said contract.
In fifth place, the investigated party provides notification to the AEPD of the breaches of
security dates 06/28/2019 and 10/31/2019.
Lastly, the respondent reports on the new scenario of co-responsibility in
the treatments as indicated in article 26 of the RGPD by the DTSPD.
Of the actions carried out in this procedure and the documentation
in the file, the following have been accredited:
PROVEN FACTS
FIRST: On January 14, 2020, the Subdirectorate General for Nationality
and Civil Status (hereinafter, SGNEC) attached to the General Directorate of Registries and
of Notaries (currently the General Directorate of Legal Security and Public Faith, in
hereinafter, DGSJFP) currently organically and functionally dependent on the
General Secretariat for the Innovation and Quality of the Public Service of Justice (in
hereinafter, SGICSPJ) of the Ministry of Justice, notifies this Spanish Agency of
Data Protection (hereinafter, AEPD) a data security breach
dates dated 11/22/2019 after becoming aware through an email
electronically by a citizen of a notification of granting of the
Spanish nationality corresponding to another person (treatment related to the
application ***APPLICATION.1).
SECOND: The notified security breach reaches 34 affected and
later they incorporated another 2 more, up to 36, all of them related to resolutions

of nationality improperly notified to third parties. The security breach

It was communicated to the interested parties on 01/16/2020.

THIRD: The security breach had its technical origin in a modification in the

process of generating resolutions granting nationality by residence

that had been made in the application ***APPLICATION.1, for processing

nationality files by residence, on ***DATE.1.

FOURTH: The fault detected originated when attaching the birth certificate of the

nationality applicant to the nationality granting resolution document

as a consequence of the high number of resolutions generated in an

concurrent.

FIFTH: The personal data affected in the security breach would correspond

to the NIE (Foreigner Identification Number), name, surnames, place and date of

birth, address at the time of submitting the application, the granting of

nationality and a copy of the birth certificate (in which the data appears again)

date and place of birth and name and surname of the parents).

SIXTH: It is stated that the SGNEC, organically dependent on the SGICSPJ, has

registered two other personal data security incidents, on dates

06/28/2019 and 10/31/2019, also with incorrect notifications due to error

recipients when communicating concessions of nationality, with 11 and 70 people

affected respectively and already solved. These security breaches were

duly notified to the AEPD but there is no evidence that they were communicated to the

affected.

SEVENTH: It is recorded, on 09/05/2018, the AEPD issued a procedural resolution sanctioning reference AP/00049/2018, in which it was sanctioned for the same facts to those now investigated to the General Directorate of Registries and Notaries dependent on the Undersecretary of Justice (now DGSJFP, dependent on of the SGICSPJ). Specifically, in the aforementioned sanctioning file it was accredited and thus it is stated in the proven facts that "The Information Technology Division and Communications of the Ministry of Justice reported that the service did not contemplate the concurrence and made a mistake when composing the birth certificate.

EIGHTH: Regarding the treatments carried out by the SGNEC, there is evidence of carried out a DPIA (data protection impact assessment) in June of 2019, which contains a risk analysis (RA) associated with data processing which manages. However, there is no update of the AR and EIDP in the modifications of the treatments carried out on 11/22/2019 that gave rise to the security breach of that date. However, in arguments the proposal of resolution provides the appropriate update to the RGPD, LOPDGDD and ENS of the treatments carried out by the investigated as well as the implantation of the corrective measures both active and proactive to avoid repetition in the future of similar events.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the General Regulation for the Protection of Data (hereinafter RGPD) recognizes each control authority, and according to what established in articles 47 and 48 of the Organic Law on Data Protection and Guarantee of Digital Rights (hereinafter LOPDGDD), the Director of the Agency Spanish Data Protection is competent to initiate and resolve this

process.

II

Definitions:

Article 4.12 of the RGPD, “violation of the security of personal data”: any

breach of security resulting in accidental destruction, loss, or alteration

or illicit of personal data transmitted, conserved or treated in another way, or the

unauthorized communication or access to said data.

Article 4.7 of the RGPD, “responsible for the treatment” or “responsible”: the person

physical or legal entity, public authority, service or other body that, alone or together with

others, determine the purposes and means of the treatment; if the law of the Union or of the

Member States determines the purposes and means of processing, the data controller

treatment or the specific criteria for their appointment may be established by the

Law of the Union or of the Member States”.

III

In the present case, in accordance with the provisions of the aforementioned article 4.7 of the RGPD and in the RD

453/2020, of March 10, which develops the basic organic structure of the

Ministry of Justice, article 3.1, corresponds to the SGICSPJ the direction, impulse and

management of the ministerial powers related to civil status and nationality, to

through the DGSJFP (art 7.1.b) of the aforementioned RD) that processes and resolves the files

Nationality.

Consequently, currently the SGICSPJ is responsible for the processing

of personal data in all the actions carried out by the different

organic units attached to it relating to marital status and nationality, whenever

that, as stated in article 4.7 of the aforementioned RGPD, is the natural or legal person,

public authority, service or other body which, alone or jointly with others, determines the

purposes and means of the treatment, in coherence with the provisions of article 3 of the aforementioned RD

453/2020 by which the SGICSPJ is responsible for the "direction, promotion and management of the

ministerial powers relating to marital status and nationality…".

It should be noted that although the General Secretariat for Innovation and Quality of the

Public Service of Justice was not responsible for data processing now

analyzed at the time of the security breach(es) (from dates

06/28/2019, 10/31/2019 and 11/22/2019), it is true that with the current basic structure of the

The Ministry of Justice is responsible for carrying out the mandatory regularizations in the

data processing for which it is responsible and promote with due diligence

its adaptation to the RGPD.

IV

Article 5.1.f) of the RGPD, Principles related to treatment, states the following:

"1. The personal data will be:

(…)

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

including protection against unauthorized or unlawful processing and against

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

or appropriate organizational ("integrity and confidentiality").

In the present case, the security breach must be qualified as integrity and

confidentiality as a consequence, in the first place, of the lack of security

adequate and appropriate technical or organizational measures (integrity), and secondly

place for unauthorized access to personal data by third parties outside

(confidentiality), both principles regulated in the same article 5.1.f) of the RGPD

above transcribed.

Article 25 of the RGPD establishes the following:

v

“Data protection by design and by default

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

scope, context and purposes of the treatment, as well as the risks of different probability and

seriousness that the treatment entails for the rights and freedoms of individuals

physical data, the data controller will apply, both at the time of determining the

means of treatment as well as at the time of the treatment itself, technical measures and

appropriate organizational arrangements, such as pseudonymization, designed to apply

enforce data protection principles, such as data minimization, and

integrate the necessary guarantees in the treatment, in order to meet the requirements of the

this Regulation and protect the rights of the interested parties.

2. The data controller will apply the technical and organizational measures

with a view to guaranteeing that, by default, they are only processed

the personal data that is necessary for each of the specific purposes of the

treatment. This obligation will apply to the amount of personal data collected, to

the extension of its treatment, its conservation period and its accessibility. Such

measures shall in particular ensure that, by default, personal data is not

accessible, without the intervention of the person, to an indeterminate number of people

physical.

3. An approved certification mechanism may be used under Article 42

as an element that proves compliance with the obligations established in the

sections 1 and 2 of this article".

In this sense, and regarding the allegation that the security breach that

gave rise to sanctioning procedure AP/00049/2018 (resolved on 09/05/2018) was

corresponds to "completely different data processing", it should be noted that

the origin of the analyzed gaps has a common cause in the lack of foresight since

the design of the concurrency factor in the processes of both applications

(***APPLICATION.2 and ***APPLICATION.1).

Article 32 of the RGPD establishes the following:

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

nature, scope, context and purposes of the treatment, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical measures and

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

which in your case includes, among others:

a) pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore the availability and access to the personal data of

quickly in the event of a 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 security level, particular account shall be taken of

takes into account the risks presented by the processing of data, in particular as

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

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data.

Article 34.1 of the RGPD establishes the following:

"1. When it is likely that the personal data breach

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

responsible for the treatment will communicate it to the interested party without undue delay."

Regarding article 32, it is clear that the data controller did not apply the

appropriate technical and organizational measures to ensure a level of security

appropriate to risk; risk that was not even evaluated in the update of the new

version of the application ***APPLICATION.1.

Regarding article 34, it should be noted that the actions carried out

It follows that the SGICSPJ, through the SGNEC, notified this AEPD of the breach of

security of personal data dated *** DATE.1 and communicated it to the interested parties

on 01/16/2020. However, the investigated also affirms that there were two breaches of

security similar and previous to the one now investigated. It appears in the allegations to the

resolution proposal that the gaps of dates 06/26/2019 and 10/31/2019 were

notified to this AEPD (art 33 RGPD) but there is no evidence that they have been communicated to

the interested parties (art 34 RGPD), although in the first it is stated in the notification that

communicated to the interested parties but it does not appear to have been carried out and, in the second, it is stated that

The interested parties were notified by telephone but it is not recorded as having been carried out.

SAW

Article 24 of the RGPD, responsibility of the person in charge of the treatment, indicates the

Next:

"1. Taking into account the nature, scope, context and purposes of the treatment,

as well as the risks of varying probability and severity for the rights and

freedoms of natural persons, the data controller will apply measures

appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the

processing is in accordance with this Regulation. These measures will be reviewed and

will update when necessary.

2. When they are provided in relation to treatment activities, between

the measures mentioned in paragraph 1 shall include the application, by the

responsible for the treatment, of the appropriate data protection policies" (…).

7th

From the facts described, it is clear that the SGICSPJ, as responsible for the

treatments now analyzed and through their organs hierarchically

dependents, did not apply the appropriate technical and organizational measures to

guarantee a level of security appropriate to the risk, since it is accredited

that outside third parties had access to information reserved to the interested party (applicant

of Spanish nationality) as a consequence of the malfunction in the start-up

production of the new version of the application ***APPLICATION.1 that manages the

DGSJFP through the SGNEC, both hierarchically dependent on the SGICSPJ.

The risks in the treatment contemplated in the new version of the application

***APPLICATION.1 should have been taken into account and evaluated by the person in charge of the

treatment (SGICSPJ) through the mandatory risk analysis and, where appropriate,

impact assessment and, based on it, have established the measures

technical and organizational that would have prevented the loss of control of the data

of applicants for Spanish nationality as a result of the

reiterated and already known lack of anticipation of concurrent processes in the treatment

of data from the different applications (APLIACIÓN.1 and APLIACIÓN.2).

It must be insisted that the level of risk and the impact were already known with

in advance, since there is a sanction file in this AEPD for acts

similar (AP/00049/2018 and resolution date on 09/05/2018) and, in addition, the SGNEC

indicates that similar events were recorded on dates prior to the security breach

dated 11/22/2019, specifically on dates 06/28/2019 and 10/31/2019.

It is also stated in the aforementioned prior sanctioning procedure that the current DTSPD

informed the SGNEC that "the service did not contemplate the concurrence and was wrong to

compose the birth certificate…" and yet a year later it was repeated

on three other occasions faithfully the incident for the same cause.

The consequence of this absence in the control of data processing from the

design and by default (art 25 RGPD) and the implementation of security measures

appropriate (art 32 RGPD) to the risk of the new version of the application

***APPLICATION.1 causing the date gap ***DATE.1, was the loss of

integrity and confidentiality of personal data, violating the two principles

collected in article 5.1.f) of the RGPD.

Article 83.4 of the RGPD provides the following:

viii

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

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

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

global total annual turnover of the previous financial year, opting for

the largest amount:

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

39, 42 and 43;"

In the present case, articles 25, 32 and 34 of the RGPD, typified

in article 83.4 of the RGPD transcribed above.

Article 83.5 of the RGPD provides the following:

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

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

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

global total annual turnover of the previous financial year, opting for

the largest amount:

a)

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

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

In the present case, article 5.1.f) of the RGPD is again violated, this

once referred to the principle of confidentiality, for which the classification

that indicates article 83.5 of the RGPD transcribed above.

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

following: Violations constitute the acts and conducts referred to in the

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.

Establishes article 72 of the LOPDGDD, under the rubric of infractions considered

very serious, the following: “1. Based on the provisions of article 83.5 of the

Regulation (EU) 2016/679 are considered very serious and will expire after three years

infractions that suppose a substantial violation of the articles

mentioned therein and, in particular, the following:

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

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

It establishes article 73 of the LOPDGDD, under the heading "Infringements considered

serious”, the following: “1. Based on the provisions of article 83.4 of the

Regulation (EU) 2016/679 are considered serious and will prescribe after two years the

infractions that suppose a substantial violation of the mentioned articles

in that and, in particular, the following:

(…)

d) The lack of adoption of those technical and organizational measures that result

appropriate to effectively apply the principles of data protection from

the design, as well as the non-integration of the necessary guarantees in the treatment, in

the terms required by article 25 of Regulation (EU) 2016/679.

(…)

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.

g) The breach, as a consequence of the lack of due diligence, of the

technical and organizational measures that have been implemented as required

by article 32.1 of Regulation (EU) 2016/679.

(…)

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

Article 33 of Regulation (EU) 2016/679

(…)

t) The processing of personal data without having carried out the evaluation of the

impact of processing operations on the protection of personal data in

assumptions in which it is required. (…)". This section, in relation to the

changes made on ***DATE.1 in the application ***APPLICATION.1.

It establishes article 74 of the LOPDGDD, under the heading "Infringements considered

minor", the following: "They are considered minor and the remaining ones will expire after a year.

infractions of a merely formal nature of the articles mentioned in the

paragraphs 4 and 5 of article 83 of Regulation (EU) 2016/679 and, in particular, the

following:

(…)

ñ) Failure to comply with the duty to notify the affected party of a violation of the

data security that entails a high risk for the rights and freedoms of users

affected, as required by article 34 of Regulation (EU) 2016/679,

unless the provisions of article 73 s) of this organic law are applicable".

From all of the above, the following can be concluded:

Regarding the classification of infractions of article 83.5.a) of the RGPD

- Violation of the principle of confidentiality (art 5.1.f) RGPD), is considered

very serious infraction for purposes of prescription (three years) as indicated in article

72.1.a) of the LOPGDD, punishable by a warning as provided in article 77.2

of the LOPDGDD.

Regarding the classification of infractions of article 83.4.a) of the RGPD

- Lack of diligence in implementing data protection by design

(art 25 RGPD in relation to article 5.1.f) of the RGPD), the absence,

violation lack of due diligence in the application of security measures

according to the risk (art 32 RGPD in relation to article 5.1.f) of the

RGPD), are considered serious infractions for prescription purposes (two years)

as stated in article 73.d), f), g) and t), of the LOPGDD and punishable with

warning according to article 77.2 of the LOPDGDD.

- The lack of communication to the interested parties of the security breach date

06/28/2020 and dated 10/31/2019 (article 34 of the RGPD in relation to article

5.1.f) of the RGPD) considered minor infringement for prescription purposes (one year)

as stated in article 74.ñ) of the LOPGDD and punishable with a warning

according to article 77.2 of the LOPDGDD.

Consequently, the violation of both principles (integrity and confidentiality)

they constitute the element of culpability that requires the imposition of a sanction.

It must be insisted that the absence of consideration of the risk already known and

previously sanctioned by this AEPD in the aforementioned sanctioning procedure

(AP/00049/2018) and after both security breaches prior to the current date

06/28/2019 and 10/31/2019, has again led to improper access by third parties

unrelated to the personal data of the interested party and repeatedly affecting the

principles of integrity and confidentiality, aggravates the reproach of guilt and

sanctioning the conduct carried out by the SGICSPJ.

Article 58.2 of the RGPD establishes the following:

IX

2. Each supervisory authority will have all of the following powers

corrections listed below:

(…)

b) sanction any person responsible or in charge of the treatment with

warning when the processing operations have violated the provisions of

this Regulation;

Establishes article 76 of the LOPDGDD under the heading "Sanctions and measures

correctives", the following:

1. The penalties provided for in sections 4, 5 and 6 of article 83 of the Regulation

(EU) 2016/679 will be applied taking into account the graduation criteria

established in section 2 of the aforementioned article.

(…)

3. It will be possible, complementary or alternatively, the adoption, when appropriate, of

the remaining corrective measures referred to in article 83.2 of the Regulation

(EU) 2016/679.

However, the LOPDGDD in its article 77, Regime applicable to certain

categories of controllers or processors, establishes the following:

X

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

who are responsible or in charge:

(…)

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

autonomous and the entities that make up the Local Administration.

(…)

2. When those responsible or in charge listed in section 1 committed

any of the infractions referred to in articles 72 to 74 of this law

organic, the data protection authority that is competent will dictate

resolution sanctioning them with a warning. The resolution will establish

also the measures that should be adopted to stop the behavior or correct it.

the effects of the infraction that had been committed.

The resolution will be notified to the person in charge or in charge of the treatment, to the body of the

that depends hierarchically, where appropriate, and to those affected who had the condition

interested party, if any.

3. Without prejudice to what is established in the previous section, the data protection authority

data will also propose the initiation of disciplinary actions when there are

sufficient evidence for it. In this case, the procedure and the sanctions to be applied

will be those established in the legislation on disciplinary or sanctioning regime that

result of application.

Likewise, when the infractions are attributable to authorities and managers, and

proves the existence of technical reports or recommendations for the treatment that

had not been duly attended to, in the resolution imposing the

The sanction will include a reprimand with the name of the responsible position and

will order the publication in the Official State or Autonomous Gazette that

correspond.

4. The data protection authority must be notified of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

5. They will be communicated to the Ombudsman or, where appropriate, to similar institutions

of the autonomous communities the actions carried out and the resolutions issued

under this article.

6. When the competent authority is the Spanish Data Protection Agency,

this will publish on its website with due separation the resolutions referring to

the entities of section 1 of this article, with express indication of the identity

of the person in charge or in charge of the treatment that had committed the infraction.

When the competence corresponds to a regional authority for the protection of

data will be, in terms of the publicity of these resolutions, to what your

specific regulations".

Of the evidence that is available according to the proven facts in the

present sanctioning procedure, is accredited by the person in charge (the

SGICSPJ) violation of the provisions of articles 5.1.f) and 25, 32 and 34 in relation to

5.1.f) of the RGPD in the terms described above.

In the alleged object of this procedure, it is considered that the

appropriate measures to prevent a recurrence of the security incident

referred to, so the person responsible for the adoption of new measures is not required.

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

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

Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE the GENERAL SECRETARIAT FOR INNOVATION AND

QUALITY OF THE PUBLIC SERVICE OF JUSTICE, with NIF S2813610I, by:

Infringement of article 5.1.f) of the RGPD typified in article 83.5.a) of the RGPD

with a penalty of warning.

1.

two.

Infringement of articles 25 and 32 of the RGPD in relation to article 5.1.f)

of the RGPD, typified in article 83.4.a) of the RGPD with sanction of

warning.

3.

Infringement of article 34 of the RGPD in relation to article 5.1.f) of the RGPD,

typified in article 83.4.a) of the RGPD, with a penalty of warning.

SECOND: NOTIFY this resolution to the GENERAL SECRETARIAT FOR

THE INNOVATION AND QUALITY OF THE PUBLIC SERVICE OF JUSTICE, with NIF

S2813610I.

THIRD

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

: COMMUNICATE this resolution to the Ombudsman,

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

This Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the Interested parties may optionally file an appeal for reconsideration before the Director of the Spanish Agency for Data Protection within a month from counting from the day following the notification of this resolution or directly contentious-administrative appeal before the Contentious-Administrative Chamber of the National Court, in accordance with the provisions of article 25 and section 5 of the fourth additional provision of Law 29/1998, of July 13, regulating the Contentious-administrative jurisdiction, within a period of two months from the day following the notification of this act, as provided in article 46.1 of the aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP, may provisionally suspend the firm resolution in administrative proceedings if the The interested party expresses his intention to file a contentious-administrative appeal. If this is the case, the interested party must formally communicate this fact by writing addressed to the Spanish Agency for Data Protection, presenting it through Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other registers provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the documentation proving the effective filing of the contentious appeal-administrative. If the Agency was not aware of the filing of the appeal contentious-administrative within a period of two months from the day following the notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es