 File No.: PS/00297/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: Dated 03/25/2019, A.A.A. (hereinafter, the claimant), filed

claim before the Spanish Data Protection Agency. The claim is

directed against the MINISTRY OF FOREIGN AFFAIRS AND COOPERATION,

currently, MINISTRY OF FOREIGN AFFAIRS, EUROPEAN UNION AND

COOPERATION, with CIF *** CIF.1 (hereinafter, MAEC, the Ministry or the entity

claimed). The reasons on which the claim is based are, in short: the treatment of

your data, without your consent, within the framework of the “***PROGRAMA.1” program, which

includes sending text messages (SMS) to mobile telephone terminals with

information on consulates, which materializes when a Spanish citizen

crosses the Spanish border; and for not having responded to the requests made

before the MAEC to delete their personal data from the file used by

said Ministry to send consular information associated with the aforementioned program,

way to stop sending these messages. According to the complainant, the requests

were processed on dates 04/24 and 09/05/18, without in any case receiving

any answer.

Likewise, he warns that he contacted his telephony operator by telephone and that

he informed him that he is not involved in the matter, that he uses a Ministry file.

Among other things, the claimant provides the following documentation:

. Copy of a letter dated 04/24/2018, addressed to the claimed entity. In this

written there is a stamp corresponding to its presentation in the Service of

Mail on the same date indicated.

He refers to a piece of news about the activities of the aforementioned Ministry, published on 10/26/2015, regarding the program "***PROGRAMA.1": "… an information service free for the citizen who travels from Spain abroad, the result of a job together with Telefónica and Orange. When the clients of these operators travel to the abroad, they will receive an SMS on their phone with the cities of that country where there are Embassy and Consulates of Spain and their corresponding emergency numbers consular The service will be activated upon arrival in the country of destination, through the roaming roaming".

In this writing, the claimant indicates his mobile telephone number and the entity with which that operates and requests that no notice be sent from the "MAEC.info" service, either to through SMS or other means, whenever the operator warns of the "Roaming" service,

and be deleted from the program "***PROGRAM.1". expressly requests that the The requested Ministry assumes the necessary steps to formalize this request.

Provides screen printing with an SMS received from "MAEC.info", from "29 de March". The recipient telephone number of this SMS does not appear. The text of this message is as follows:

"***PROGRAM.1. In case of consular emergency call Consulates in Paris… (no. phone number), Bayonne (phone number)".

. Copy of a letter dated 09/05/2018, addressed to the MAEC. In this writing there is a stamp corresponding to its presentation at the Postal Service in the

same date indicated.

The content of this writing is basically similar to the previous one. Repeat your request

to not receive SMS from the repeated program “***PROGRAMA.1” and the cancellation of your

data in the file used for this purpose or any other similar file of the MAEC. request

expressly be informed about it.

SECOND: On 05/17/2019, the claim was transferred to the entity

claimed, in accordance with the provisions of article 65.4 of the Organic Law

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

digital rights (hereinafter, LOPDGDD), in order to proceed to its analysis,

notify the claimant of the decision adopted and provide this Agency with information

about.

On 07/08/2019 and 08/01/2019, the MAEC responded to the aforementioned transfer stating

that the claimant receives an SMS on his mobile terminal when he travels abroad as

consequence of an agreement signed by the Ministry with certain companies

telephone operators; although it does not request, store or treat the data of the

citizens who travel abroad in order to send said SMS, but

It is these operators that have your personal data.

Thus, not being the holder of the claimant's data, the claimed party considers that it does not

no communication should be sent to you. You understand that the exercise of your rights

You must request it from the operator.

The aforementioned entity, on 08/01/2019, sent this Agency a copy of the

communication addressed to the claimant on the occasion of the claim made. In

this communication, dated 07/22/2019, the MAEC informs the claimant that the SMS

of the program “***PROGRAMA.1” is sent as a result of an agreement that

that Ministry signed with various telephone operators. Also, it is indicated that

has the data of Spanish citizens who travel abroad, nor does the

mobile number, unless they voluntarily enroll in the Registration application

of Travelers. Finally, the claimant is warned that "if you do not wish to receive the referrals

SMS when traveling abroad, you must request it from your telephone operator as it is

holder of your personal data and your mobile number".

THIRD: Once the reasons stated by the claimed party in its

response to the transfer, it was considered that the initiation of a procedure

sanctioning party having been attended to the claim in accordance with the provisions of the

article 65.4 of the LOPDGDD, and a resolution dated 09/09/2019 was issued, agreeing on the

file of the examined claim.

On 10/03/2019, the claimant filed an appeal for reconsideration, stating that

the telephone operator sends information arranged by the Ministry and that

it is up to the latter to warn the operators that a specific interested party does not wish to

receive the information object of the program "***PROGRAMA.1", that is, about the

right of opposition exercised. He adds that it is the Ministry that must deal with the

citizen's claim.

This resource was estimated by resolution of 07/10/2020, in which it was agreed, in

Consequently, admit the claim filed against the MAEC for processing.

FOURTH: In view of the facts denounced in the claim and the

documents provided by the claimant, the Subdirectorate General for Inspection of

Data proceeded to carry out preliminary investigation actions for the

clarification of the facts in question, by virtue of the investigative powers

granted to the control authorities in article 57.1 of the Regulation (EU)
2016/679 (General Data Protection Regulation, hereinafter RGPD), and
in accordance with the provisions of Title VII, Chapter I, Second Section, of the
LOPDGDD.

The Inspection Services of this Agency requested the MAEC the agreement of the
service subscribed with the operators Telefónica de España, S.A. and Orange Spain,
S.A.U., or any others with whom this service has been agreed. With date
03/26/2021 a reply was received in which it states that they do not appear in
the archives of that Ministry no Convention or Agreement signed with the aforementioned
operators, nor with any other, nor any other written document related to the
"***PROGRAM.1" campaign.

Requested information on the repeated agreements with various operators,
received in this Agency the following answers:

a) On 05/11/2021, the operator Xfera Móviles, S.A. He stated that he did not
participate in the aforementioned program, nor is it a service that they provide
Independent.

b) On 05/18/2021, the entity Orange Espagne, S.A.U. reported that the
program "***PROGRAMA.1" emerged on 10/26/2015 at the initiative of the MAEC, which
requested the collaboration of the operators, and consists of sending text messages
information to roaming customers when connecting to a foreign network with
roaming agreement. Specifically, it is an initiative that was led by the
Consular Emergency Unit of the MAEC, as published on the page
Ministry website (indicates the link).

The roaming service is activated by default in the Orange Spain rate,
S.A.U. but the user can deactivate the roaming service and therefore not
the informative SMS of the program "***PROGRAMA.1" would be received.

The content of the text messages was defined by the MAEC itself, which appears

as their sender.

The service is still active and is regularly updated by referring to the

operators of an Excel file with updated information.

It adds that there is no document in the databases of that company that

formalize the aforementioned initiative.

With this response, he provided:

- Screen printing of several consular emergency SMS, in which

checks that the sender of the message is the MAEC, appearing as such

“MAEC-info”.

- Email dated 12/21/2020, sent by the IT area of the MAEC,

with an update to data from Manchester and Sierra Leone.

c) On 06/08/2021, Telefónica de España, S.A. stated that the service

“***PROGRAMA.1” is a free information service for citizens provided

by the MAEC, in collaboration with Telefónica de España, S.A. and Orange Spain,

S.A.U., according to a press release from the aforementioned Ministry on 10/26/2015 (indicates link).

It states that the sender of the SMS is the Ministry itself, as can be seen in the

example provided (“FROM: ***EMAIL.1: in case of consular emergency call

Embassy… More info www.exteriores.gob.es”).

At the request of the Ministry, it integrated the sending of these messages in the platform of

messaging of Telefónica de España, S.A., already existing, within the framework of the

relationship he had with said Ministry for the provision of various services.

It ends by adding that the Embassies or Consulates have the power to act

in consular emergency situations, such as arrests, issuance of documents

emergency travel to return to Spain, help contact relatives and

friends, or assist in case of catastrophes, for which purpose this service was developed in

collaboration with Telefónica de España, S.A.

Telefónica de España, S.A., which was expressly requested, did not provide any

document formalizing the Ministry's initiative with this operator.

FIFTH: On 07/05/2021, the Director of the Spanish Agency for the Protection of

Data agreed to initiate a sanctioning procedure against the MAEC entity, in accordance with the

provided in articles 63 and 64 of Law 39/2015, of October 1, of the

Common Administrative Procedure of Public Administrations (hereinafter,

LPACAP), for alleged violations of articles 21 and 28.3 of the RGPD,

typified, respectively, in articles 83.5.b) and 83.4.a) of the RGPD.

In the same agreement to open the procedure, it was warned that the infractions

imputed, if confirmed, may lead to the imposition of measures, in accordance

with the provisions of the aforementioned article 58.2 d) of the RGPD.

SIXTH: Once notified of the aforementioned initial agreement, the MAEC presented a written

allegations in which he requests the file of the sanctioning procedure of

accordance with the following considerations:

. The initiative "***PROGRAMA.1" derives from the obligations that consular assistance

imposes on the claimed (article 2.2.i) of Law 20/2014, of March 25, of the action and the foreign service; Vienna Convention on Consular Relations of 04/23/1963; and article 23 of the Treaty on the Functioning of the European Union).

. In 2015, when the collaboration of the MAEC with the operators Telefónica de España, S.A.U. and Orange Spain, S.A.U. for development of the aforementioned initiative, Law 40/2015, of October 1, of Legal Regime of the Public Sector (LRJSP) nor the RGPD.

. The claimant has not proven having received information about consulates in his mobile terminal (the documentation provided does not include the telephone line number recipient of the SMS to which it refers).

. Personal data remains in the custody of the telephone companies, without that the MAEC carry out any data processing that conforms to the definition collected in article 4.2 of the RGPD. Therefore, the Ministry cannot be considered as responsible for the treatment, since it does not request, collect, store, access or treats the data of the citizens who are clients of the telephone operators, nor does it know their identity.

Thus, the MAEC has not provided at any time the name and number of claimant's telephone number, so it is not possible to "unsubscribe" the applicant from any file, as there is none that collects the identity, telephone number and travel plans of the citizens who travel abroad with a mobile phone that works in Spain.

. Nor is the MAEC the sender of the messages, which lacks the facilities technology to do so and has no way of detecting when a client of the telephone operators use data networks when roaming. The senders are telephone companies, which transfer the information provided by the MAEC, simultaneously with other SMS related to the use and tariffs of the services telephony, voice calls or mobile data usage while roaming.

. The MAEC cannot be sanctioned for not having signed the agreement regulated in the

article 28 of the RGPD, because it was not in force in 2015 and because said

agreement is not applicable, since the MAEC is not in charge of data processing

personal on behalf of the person in charge. The MAEC has not and will not have

such personal data, does not receive them from the companies participating in the initiative nor

treat on their behalf.

Currently this collaboration must be formalized through an agreement

administrative, of those regulated in articles 47 and following of the LRJSP, but not

from a data protection perspective.

. Corresponds to the telephone operators, at the time of data collection

of its clients, inform them of the purpose of the treatment, request their

consent to receive communications and indicate the way to exercise the

rights that assist them. Consequently, the right to oppose to receive the

SMS referrals must be exercised by the claimant before the telephone operator with the

that has contracted its services, which is the owner and performs the treatment of

your personal data, and to which it corresponds to process the opposition.

SEVENTH: On 10/22/2021, a resolution proposal was formulated in the sense

Next:

1. That the Director of the Spanish Agency for Data Protection sanction

warning the MAEC entity, for infractions of articles 21 and 28.3

of the RGPD, typified in articles 83.5.b) and 83.4.a) of the same Regulation, and

classified as very serious and serious for prescription purposes in articles 72.1.k) and

73.k) of the LOPDGDD, respectively.

2. That the Director of the AEPD requires the claimed entity so that, in the

term to be determined, adopt the necessary measures to adapt its actions to

the personal data protection regulations, with the scope expressed in the

Fundamentals of Rights of the proposed resolution.

EIGHTH: Once the requested entity has been notified of the aforementioned resolution proposal,

receives a letter from the same in which it requests the file of the sanctioning procedure

without imposing measures or requiring only the formalization of an agreement

in accordance with the provisions of article 28.3 of the RGPD, since the MAEC entity

does not have the status of controller of the treatment of the program "***PROGRAMA.1"

and has not incurred in fraud or negligence, having followed a reasonable interpretation of the

rule.

The aforementioned entity bases its request on the following considerations:

1. The AEPD considers that the MAEC is the one who decides the ends and means of the

treatment that requires the application of the program "***PROGRAMA.1" and that this is

sufficient, in its opinion, for it to have the status of data controller, even

when you have not collected, nor do you have, nor have you ever had, access to the data that is

treat.

Faced with the considerations of the AEPD, it indicates that article 4 of the RGPD defines the

responsible for the treatment as the one who determines its purposes and means, without making

express mention of whether or not you have access to the data being processed.

He understands that, in this case, the Ministry defines the purposes (assistance to the Spanish

abroad), but it does not decide the means used (an SMS that is sent to

customers of the operators who have activated the roaming of their data together with the

rest of the messages of the operators themselves) for the fulfillment of the purpose (that the

assistance message from the MAEC reaches Spaniards abroad). The fact of

that the Ministry communicates to the operators the information that must be transmitted, in

"excel" format, is aimed at fulfilling the intended purpose, but does not imply that the

MAEC decides the means, which rather seem decided by the operators of

telephony, which use the same channel they use for the referral of other

messages to your customers at the same time.

2. The MAEC does not have the status of data controller because it does not agree

to the personal data processed. This entity does not share the interpretation of the

AEPD in this regard, based on an assumption of data processing for

advertising and in a case of provision of services in accordance with Law 9/2017, of 8

November, of public sector contracts (LCSP).

Understands that resolving this issue, not provided for in the standard, requires a

interpretation, as evidenced by the fact that the AEPD bases its position on the

reports and guidelines mentioned in the motion for a resolution; and what to have

acted in accordance with the reasonable interpretation defended by the MAEC does not allow

appreciate any negligence or the concurrence of the subjective element of the

guilt, essential for the imposition of a sanction.

In the opinion of the MAEC, the application of the interpretation criteria of the norms that

contained in article 3 of the Civil Code would allow reaching the opposite conclusion to the

proposed by the AEPD, as set out below:

a) There is no rule that establishes that the data controller will be with

regardless of whether you have or have had access at any time to the data

treated.

b) Against this, there are provisions in the RGPD that presuppose that the person responsible for the

treatment has or has had access to the data, without prejudice to the fact that it may order

his treatment of others. Thus, the following forecasts can be mentioned:

. The MAEC, which does not collect the data, is not in a position to comply with the

obligations established in articles 13 and 14 of the RGPD, provided for the

time the data is collected. According to these articles, which identify the

responsible for the treatment with whom it collects the data, the MAEC should comply

those obligations when a company collects data from a new customer.

. The MAEC cannot enforce the rights of the interested parties, so

should transfer those requests to the telephone operators.

. Article 28.3 of the RGPD provides that the contract or legal act that binds the

responsible for the treatment and the person in charge establishes the obligation of the latter to

Delete or return the data to the person in charge once the provision of the service has ended.

service. This allows us to understand that the person responsible is the one who has in his possession the

data and/or has power of disposal over them. Only in this case can

It is understood that its return or suppression proceeds.

c) Report 0007/2019 of the Legal Office of the AEPD and the Judgment of the Chamber of

the contentious-administrative of the Supreme Court 772, referring to assumptions

special (contractor in charge of treatment, in the first case, and treatment of

data for advertising purposes, in the second), configure the access and even the

ownership of the databases as a determining element of holding the

condition of data controller, the contrary conclusion being applicable only

in the specific cases contemplated (public procurement and treatment of

data for advertising purposes). This is what results from his analysis, in the way in which he exposes

next:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

. The aforementioned Report 0007/2019, which deals with the correct interpretation of what

provided in article 33.2 of the LOPDPGDD, refers to a case of

data processing commissioned by a Public Administration within the framework of the

LCSP and determines if the entities that act as concessionaires

Administrative staff in public services have the status of being in charge or

responsible for the treatments.

According to the MAEC, this report contains considerations that support the

identification of the person in charge of the treatment with the person in charge of the file in the

that the data is hosted, such as the one that indicates that access to the data by

of the manager for the provision of the service is not a data communication, which

which presupposes that the controller is the one in possession of the data (if what

What you want to avoid is that it is legally configured as a transfer of data, which

that materially it is, it is because it is assumed that the person responsible is the one

is in the power of the data); or when it is indicated that the person in charge will be deemed to

is responsible if it uses for its own purposes the data that has been communicated to it (the

reference to the data that the person in charge has communicated presupposes the

prior communication of the data by the person in charge and, therefore, that they are in their

can).

In the present case, there is no such communication because the MAEC does not have, nor has

never had access to customer data from telephone companies.

These are the ones that collect the data of their clients and those that have access to

they.

In any case, the AEPD report 0007/2020 represents an exception to the

general regime of conceptuación of the person in charge of the treatment; not transferable

to a different assumption such as the one analyzed in this proceeding.

. The Supreme Court Judgment 772/2020, refers to a case of

use of databases of third-party companies to make shipments

commercial.

This Judgment is based on provisions of the regulation of protection of

data specifically referring to the processing of data for advertising purposes,

assumption different from the one now analyzed, referring to the treatment of data for the

fulfillment of a purpose of public interest. Therefore, the conclusion that

The condition of data controller and its obligation to comply will fall on the MAEC.

manage the exercise of the right of opposition of the claimant, beyond

tell you to contact your telephone operator, it would be fully justified

if we were dealing with data processing for advertising purposes, but it is not

so clear that conclusion when we are outside that scope.

d) The obligations imposed on the data controller seek to guarantee

and protect the rights of the holders of personal data, for which

It seems reasonable that all these obligations are imposed on someone who, in a way

effective has the possibility of complying with them, being certainly complex that it can

do it, at least efficiently, who does not have and has never had access to the

data. This is an interpretation in accordance with the spirit and purpose of the standard.

e) Finally, the respondent points out that the only statement about the possibility that

you have the status of data controller without having access to the data

treated is included in Directive 07/2020 of the European Committee for Data Protection

(CEPD), which is mentioned in the motion for a resolution, but it is a

statement devoid of explanation or argumentation that allows us to understand its basis;

and incompatible with that maintained by the MAEC, according to which the legislator attributes the

condition of responsible who does not have access to the data processed only in

cases of use of third-party databases to send advertising.

3. In relation to the considerations contained in the proposed resolution

regarding the infringement of article 83.5.b, for non-compliance with article 21, both

of the RGPD, reiterates the following:

a) The MAEC expressly answered the claimant's request, sending him to his

telephone operator, considering that this was the appropriate route for the role of the Ministry

in these data treatments.

b) The MAEC does not have the status of data controller, nor does it

You can exercise the right of opposition or cancellation.

c) The basis of the treatment carried out by the program "***PROGRAMA.1" is not the

marketing, as in the case contemplated in the Judgment of the Court

Supreme 772/2020, of June 15; it is reasonable to understand that the basis of treatment

of the data to apply the program "***PROGRAMA.1" would be the one foreseen in the article

6.1 e) RGDP, this is the treatment that is necessary for the fulfillment of a mission

carried out in the public interest or in the exercise of public powers vested in the

responsible for the treatment. The reason for processing the data is compliance

of a duty assumed by the State through the MAEC, of assistance to Spaniards in

the outside.

Therefore, the regulation of the right to oppose the processing of data for

commercial is not transferable to the treatment for the purpose that concerns us in this

case.

In this way, the conclusion that makes the MAEC bear the condition of responsible

of the treatment and its obligation to manage the exercise of the right of opposition of the

claimant would be justified if we were dealing with data processing for

advertising, but that conclusion is not so clear when we are outside that area.

Thus, the obligation of the data controller who entrusts the processing to an entity

that uses its own databases or those of third parties, to communicate the request to the

responsible for the file so that it meets the right of opposition of the

affected is not contemplated in any other case than that of carrying out

advertising campaigns. It is, therefore, a special rule that cannot be transferred to other

assumptions. This is the result of the literal wording of the applicable regulations, in particular the

article 51.4 GDPR.

Therefore, it can be reasonably concluded that the actions of the MAEC in referring the

concerned to your telephone operator, with which you have a contractual relationship

which is the determinant of receiving the SMS from the program "***PROGRAMA.1" when

activate the roaming of your data, does not imply any violation of article 21

GDPR.

4. The entity complained against considers the proposed sanctions of

agree with the following arguments:

a) The qualification of the MAEC as data controller should be reconsidered,

given that he does not have and has not had access at any time to the data that is processed

for purposes other than advertising, in addition to the dubious concurrence of the

requirement to define the means of treatment. On this matter, he adds that the last

Paragraph of Recital (81) of the RGPD allows us to deduce that the condition of

responsible for the treatment implies access to the data that is processed:

“(81) … Once the treatment on behalf of the person in charge has finished, the person in charge must, at

choice of the former, return or delete personal data, unless Union Law or

of the Member States applicable to the person in charge of the treatment obliges to keep the data”.

b) Even if the premises of the proposed resolution were accepted, the actions of the

MAEC has been based on a reasonable interpretation of the standard, so it cannot

neither fraud nor fault can be appreciated, and the subjective element of culpability does not concur

necessary for the imposition of a sanction, in accordance with the provisions of the

article 28 of Law 40/2015.

This is without prejudice to the convenience of formalizing an administrative agreement between the

MAEC and the telephone operators participating in the program “***PROGRAMA.1”

that collects the terms of the collaboration.

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited:

PROVEN FACTS

FIRST: On 10/26/2015, the MAEC entity ordered the development of a

program named “***PROGRAM.1”, configured as “… a service of

free information for citizens traveling from Spain abroad”, which

consists of sending an SMS to your mobile telephone terminal with the cities of that

country where there is an Embassy and Consulates of Spain and their corresponding numbers

consular emergency. This service is activated through the roaming system

“Roaming”, upon arrival in the country of destination.

For the start-up of this service, the MAEC agreed with the

operators Telefónica de España, S.A. and Orange Spain, S.A.U. what are you

entities send their clients an SMS with the information provided by the MAEC.

Customers receive this message when traveling abroad, upon arrival in the country of

destination, through the “Roaming” roaming system. information is transferred

provided by the MAEC, simultaneously with other SMS sent by the

operators related to the use and rates of telephony services, calls of

voice or mobile data usage while roaming.

SECOND: There is no record in the proceedings of any document through which

formalize the provision of the service outlined in the First Proven Fact by

of the MAEC and the entities Telefónica de España, S.A. and Orange Spain, S.A.U.

In its response to the AEPD Inspection Services, dated 03/26/2021, the

MAEC stated that there is no record in the files of that Ministry of any agreement or

agreement signed with the aforementioned operators, nor with any other, nor any other

written document related to the campaign “***PROGRAMA.1”.

On 05/18/2021, the entity Orange Espagne, S.A.U. reported that it does not appear in

the databases of that merchant a document that formalizes the initiative

“***PROGRAM.1”.

Telefónica de España, S.A., which was expressly requested, did not provide any

document formalizing the Ministry's initiative with this operator.

THIRD: The entity Orange Espagne, S.A.U. I inform the Inspection Services

of the AEPD that the service "***PROGRAMA.1" is still active and is updated

periodically by the MAEC through the referral to the operators of a

Excel file with the information to be sent by SMS.

FOURTH: It appears in the proceedings, provided by the claimant, a text message

(SMS) sent in execution of the program “***PROGRAM.1”; listed as sender

“MAEC.info”, and with the following text:

“***PROGRAM.1. In case of consular emergency call Consulates in Paris… (no.

phone number), Bayonne (phone number)”.

FIFTH: The claimant has stated before this AEPD that the entity MAEC treated

your personal data, without your consent, for sending to your telephone terminal

mobile phone for text messages in the framework of the program “***PROGRAMA.1”, with

information about consulates.

SIXTH: On 04/24/2018, the claimant sent a letter to the MAEC entity in

the one that indicates your mobile telephone number and the entity with which you operate; and requests that

no notice of the program “***PROGRAM.1” is sent every time the operator

warns of the “Roaming” service, either through SMS or other means, and be excluded

of said program. In this writing, the claimant expressly requests that the

The requested Ministry assumes the necessary steps to formalize this request.

There is no record in the proceedings of any response issued by the MAEC to this request

exercise of rights formulated by the claimant.

SEVENTH: On 09/05/2018, the claimant reiterated his request to the MAEC

above, in order not to receive SMS from the program “***PROGRAMA.1” and for the

cancellation of your data in the file used for this purpose or any other similar

MAEC. He expressly requests to be informed in this regard.

There is no record in the proceedings of any response issued by the MAEC to this request exercise of rights formulated by the claimant.

EIGHTH: On the occasion of the claim transfer process, the entity MAEC sent the claimant a response, dated 07/22/2019, in which he reports that the SMS of the program "***PROGRAMA.1" is sent as a result of an agreement that the Ministry signed with various telephone operators. Also, it indicates that does not have the data of Spanish citizens traveling abroad, nor the mobile number, unless they voluntarily enroll in the Registration application of Travelers; and warns the claimant that "if you do not want to receive the aforementioned SMS When you travel abroad, you must request it from your telephone operator as it is holder of your personal data and your mobile number".

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of control, and according to the provisions of articles 47 and 48 of the LOPDGDD, the Director of the Spanish Agency for Data Protection is competent to initiate and to resolve this procedure.

II

In this case, the fact that the program "***PROGRAM.1" is an initiative of the aforementioned Ministry, conceived as a service to the citizen that travels from Spain abroad that said entity decides to provide due to the

competences granted by the regulations that apply to it.

Nor is it controversial that the initiative and development of the aforementioned program responds to a clear public interest for the benefit of those citizens who move to the abroad, so that their legitimacy and suitability are not questioned, nor the proportionality of data processing with the intended purpose (the MAEC itself states that the legal basis of the treatment, which is not the object of analysis in these actions, is the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the data controller).

Given that the execution of the program entails carrying out data processing personal, in advance it is convenient to specify the character under which the entity MAEC intervenes in the analyzed case, from the point of view of data protection personal.

The aforementioned Ministry bases its allegations basically on denying its participation in the events as the entity responsible or in charge of the treatment, noting that it does not process the personal data of citizens who travel to the foreigner, who does not have these data, does not register them in any database or access them on behalf of the telephone operators. These are operators, in the opinion of the MAEC, those that have the personal data used for the sending of SMS that motivate the actions, which are registered

in their own files, in the custody of these companies; and they are the senders of the messages in question.

For the same reason, the Ministry understands that it corresponds to the operators mentioned request their clients' consent to receive communications, as well as how to indicate the means for the exercise of their rights and attend to requests that they formulate.

The figures of "responsible for the treatment" and "in charge of the treatment" are defined in article 4 of the RGPD as follows:

. “Responsible for the treatment or responsible: the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the ends and means of the treatment; if the law of the Union or of the Member States determines the ends and means of the treatment, the person in charge of the treatment or the specific criteria for their appointment may be established by the Law of the Union or of the Member States”.

. “In charge of the treatment or in charge: the natural or legal person, public authority, service or other body that processes personal data on behalf of the person responsible for the treatment".

Article 24 of the RGPD, referring to the "Responsibility of the person responsible for the treatment”, establishes the following:

"1. Taking into account the nature, scope, context and purposes of the treatment as well as risks of varying probability and severity to the rights and freedoms of individuals physical data, the controller will apply appropriate technical and organizational measures to in order to guarantee and be able to demonstrate that the treatment is in accordance with this Regulation. Such measures will be reviewed and updated as necessary.

2. When they are provided in relation to treatment activities, among which measures mentioned in section 1 will include the application, by the person in charge of the treatment, of the appropriate data protection policies…”.

Report 0064/2020 of the Legal Office of the AEPD has emphatically expressed that “The RGPD has meant a paradigm shift when addressing the regulation of the

right to the protection of personal data, which is based on the

principle of "accountability" or "proactive responsibility" as pointed out

repeatedly by the AEPD (Report 17/2019, among many others) and is included in the

Statement of reasons for Organic Law 3/2018, of December 5, on the Protection of

Personal data and guarantee of digital rights (LOPDGDD)".

The report goes on to say the following:

"…the criteria on how to attribute the different roles remain the same (section 11),

reiterates that these are functional concepts, which are intended to assign responsibilities

according to the actual roles of the parties (paragraph 12), which implies that in most

of the assumptions must take into account the circumstances of the specific case (case by case)

attending to their actual activities instead of the formal designation of an actor as

"responsible" or "in charge" (for example, in a contract), as well as autonomous concepts,

whose interpretation must be carried out under the European regulations on the protection of

personal data (paragraph 13), and taking into account (paragraph 24) that the need for a

factual assessment also means that the role of a controller is not

derives from the nature of an entity that is processing data but from its activities

concrete in a specific context…".

The concepts of controller and processor are not formal, but

functional and must attend to the specific case.

The data controller is from the moment it decides the purposes and

means of treatment, not losing such condition by leaving a certain margin

of action to the person in charge of the treatment or for not having access to the databases

of the manager.

This is unquestionably expressed in Guidelines 07/2020 of the European Committee for

Data Protection (CEPD) on the concepts of data controller and

manager in the RGPD:

“A data controller is one who determines the purposes and means of processing.

treatment, that is, the why and how of the treatment. The data controller must

decide on both ends and means. However, some more practical aspects of

implementation ("non-essential means") can be left to the person in charge of the

treatment. It is not necessary that the person in charge actually has access to the data that is

they are trying to qualify themselves as responsible” (the translation is ours).

Article 28.10 of the RGPD also addresses the criteria for determining the purposes

and means of treatment to establish the responsibility of the person in charge of the treatment.

treatment in the commission of infractions to the Regulation itself. according to this

article, if the person in charge determines the purposes and means of the treatment, it will be considered

responsible for it:

“10. Without prejudice to the provisions of articles 82, 83 and 84, if a data processor

infringes this Regulation when determining the purposes and means of the treatment, it will be

considered responsible for the treatment with respect to said treatment”.

In the present case, it is stated that the MAEC is responsible for data processing

now analyzed, since, as defined in article 4.7 of the RGPD, it is the

entity that determines the purpose and means of the treatments carried out. In its

The condition of data controller is obliged to comply with the provisions of

the transcribed article 24 of the RGPD and, in particular, what is related to the effective control and

continuation of the “appropriate technical and organizational measures in order to guarantee and

be able to demonstrate that the treatment is in accordance with this Regulation”, between

those found in article 28 of the RGPD in relation to the

in charge of the treatments that act in the name and on behalf of the aforementioned

Ministry.

In this sense, and in relation to the allegation made by the MAEC in its written

allegations to the initial agreement, according to which the telephone operators are the

that have the databases and, therefore, do not act as managers

but as responsible for these treatments, in the Guidelines 07/2020 of the

European Committee for Data Protection (CEPD), on the concepts of responsible

of the treatment and manager in the RGPD, it is indicated that "42. It is not necessary that the

data controller actually has access to the data being processed.

processing. Anyone who outsources a processing activity and, in doing so, has a

determining influence on the purpose and (essential) means of processing (e.g.

example, adjusting the parameters of a service in such a way as to influence whose

personal data will be processed), should be considered as responsible even if

you will never have real access to the data" (the translation is ours). The MAEC determines

who can send the messages that are the object of the program

"***PROGRAM.1" developed by the Ministry itself.

Likewise, the legal report of the AEPD dated 11/20/2019, with internal reference

0007/2019, and STS 772/2020 (for all), analyze the legal figure of person in charge of the

treatment from the perspective of the RGPD, which regulates this figure in its article 28.

The existence of a data processor depends on a decision taken by

the person in charge of the treatment, who may decide to carry out certain

treatment operations or contract all or part of the treatment with a

duty manager.

The essence of the function of the person in charge of the treatment is that the personal data

are processed in the name and on behalf of the data controller. In practice,

it is the person in charge who determines the purpose and the means, at least the essential ones,

while the person in charge of the treatment has the function of providing services to the

responsible for the treatment. In other words, “acting in the name and on behalf of

of the data controller” means that the data controller is at the

servicing the interest of the controller in carrying out a task

and that, therefore, follows the instructions established by it, at least in

what refers to the purpose and the essential means of the entrusted treatment.

The person in charge of the treatment is the one who has the obligation to guarantee the application

of the data protection regulations and the protection of the rights of the

interested, as well as being able to demonstrate it (articles 5.2, 24, 28 and 32 of the RGPD).

The control of compliance with the law extends throughout the treatment,

From the beginning to the end. The data controller must act, in

in any case, in a diligent, conscious, committed and active manner.

This mandate of the legislator is independent of whether the treatment is carried out

directly the person in charge of the treatment or that it is carried out using a

treatment manager.

In addition, the treatment carried out materially by a treatment manager for

account of the person in charge of the treatment belongs to the sphere of action of this

last, in the same way as if he did it directly himself. The person in charge of

treatment, in the case examined, is an extension of the person responsible for the

treatment.

In light of the principle of proactive responsibility (art 5.2 RGPD), the person in charge of the

treatment must be able to demonstrate that it has taken into account all the elements

provided for in the GDPR.

The data controller must take into account whether the data processor

provides adequate documentation that demonstrates said compliance, policies of

privacy protection, file management policies, privacy policies

information security, external audit reports, certifications,

management of rights exercises, etc.

Likewise, before outsourcing a treatment and in order to avoid possible violations

rights and freedoms of those affected, the data controller must

enter into a contract, other legal act or binding agreement with the other entity that

establish clear and precise data protection obligations.

The person in charge of the treatment can only carry out treatments on the instructions

documentation of the controller, unless required to do so by law

of the Union or of a Member State, which is not the case. In this regard, article 29

of the RGPD refers to the “Processing under the authority of the person in charge or the person in charge

of treatment” in the following terms:

“The person in charge of the treatment and any person acting under the authority of the person in charge

or the person in charge and has access to personal data may only process said data following

instructions of the person in charge, unless they are obliged to do so under the Law of the

Union or of the Member States.

The person in charge of the treatment also has the obligation to collaborate with the
responsible for guaranteeing the rights of the interested parties and fulfilling the obligations
of the person in charge of the treatment in accordance with the provisions of the aforementioned article 28 of the
GDPR (and related).
Therefore, the data controller must establish clear modalities for
said assistance and give precise instructions to the person in charge of the treatment on how
comply with them adequately and previously document it through a contract or
or in another (binding) agreement and check at all times of the development of the
contract its fulfillment in the manner established therein.
You will only be fully responsible when you are fully responsible
of the damages caused in terms of the rights and freedoms of the interested parties
affected. All of this, without avoiding the responsibility that may be incurred by the
responsible for the treatment in order to avoid those damages.
In the present case, the correct legal classification in accordance with the RGPD of the
telephone operators to which the MAEC commissioned the sending of the SMS object of the
program "***PROGRAMA.1" is the one in charge of the treatment, since,
act fully in the name and on behalf of the MAEC, for the benefit of this Ministry,
which is the entity responsible for the treatment for all purposes in terms of
Data Protection.
The arguments presented are considered sufficient to respond to the
allegations to the proposed resolution raised by the entity MAEC.
Without considering these arguments, the aforementioned entity alleges that it does not intervene in the
made under the condition of data controller. Although he accepts that it defines
the purposes for which personal data is processed within the framework of the program
"***PROGRAMA.1", denies that the MAEC is the entity that determines the means, that
are decided by the operators. According to the respondent, its action in this regard

it is limited to communicating to the operators the information that must be transmitted, and they are

these operators who decide to send SMS messages through them

channels they use to send other own messages to their customers in

roaming.

This Agency does not share the approach formulated by the MAEC entity.

It is the MAEC who decides to report on the situation of the Embassies and Consulates

of Spain abroad and the form of contact with these centers; and the entity that

decides the specific information to be transmitted, its specific recipients

(customers of the telephone operators with whom the execution of the program agreed

traveling abroad with roaming enabled) and how the information will be delivered.

information (SMS message).

In short, it is the MAEC that determines the data processing operations

personal to be carried out. It is the same as saying that the MAEC is the entity

which determines why (the purpose) and how (the means) personal data is processed

to achieve the intended purpose.

Regarding the “means of treatment”, Guidelines 07/2020 of the European Committee

Data Protection (CEPD) on the concepts of data controller and

manager in the RGPD, already cited, indicate the following:

“As far as the determination of the means is concerned, a distinction can be made between

essential and non-essential resources. The "essential means" are traditionally and inherently

reserved to the data controller. While non-essential media also

can be determined by the person in charge, the essential means must be determined by

the data controller. "Essential media" are media that are closely

related to the purpose and scope of the treatment, such as the type of personal data that

are processed ("what data will be processed?"), the duration of the treatment ("for how long will

will treat?"), the categories of recipients ("who will have access to them?"), and the categories

data subjects ("whose personal data is being processed"). Along with the purpose of

treatment, the essential means are also closely related to the issue

whether the treatment is legal, necessary and proportionate. "Non-essential means" refers

to more practical aspects of the application, such as choosing a particular type of

software or detailed security measures that can be left to the person in charge of the

treatment for you to decide" (the translation is ours).

There is no doubt about the condition of MAEC responsible for processing,

that is not affected by the fact that it agrees with other entities (the

telephone operators mentioned in this act) the execution of the operations of

treatment according to your instructions. It so happens that even in this

In this case, there is doubt about the status of those in charge of the treatment that should be attributed

to those operators, which are separate and independent entities of the

responsible for acting for the benefit and on behalf of the latter and according to its instructions.

These and not others are the circumstances that make up the concepts of responsible and

in charge of the treatment and the criteria for the distribution of their respective functions,

that have not changed with the approval of the RGPD.

Likewise, the MAEC reiterates that it cannot be attributed the status of responsible for the

treatment because it does not access the data, and points out in this regard that there is no standard

according to which the data controller will be regardless of whether

whether or not you have access to the personal data processed at any time.

The respondent understands that in order to resolve this issue, a

interpretation, which the AEPD bases on a case of data processing for

advertising and in a case of provision of services in accordance with the LCSP, whose

conclusions cannot be transferred to the present case, contrary to what is indicated in the

resolution proposal.

As the MAEC rightly says in its allegations, the rule does not provide whether the person responsible for the

treatment, to be, access or not the data subject to treatment. And it is so

because the RGPD already establishes as sufficient to grant that condition the fact of

that the intervening entity determines the purposes and means of the treatment, so that

no other requirement or condition can be added with interpretations of the standard

that said norm does not foresee and, even less, consider that other requirement as

preponderant to the point of annulling what the norm does establish. The result of the

interpretation made by the MAEC in its pleadings brief would give rise to a

case in which an entity determines the purposes and means of the treatment, but

is not considered responsible for the treatment for a circumstance that the RGPD does not

contemplates, as is the access or not to personal data by that entity.

The most accurate conclusion leads to understand that the entity that decides the purposes and

means of processing is responsible regardless of whether that entity accesses or

not to the personal data processed. As noted above, this is also

the position defended by the European Committee for Data Protection in the Guidelines

07/2020.

Contrary to what was stated by the aforementioned Ministry, this Agency bases its conclusion

prior to what is established in the standard and in consolidated criteria, even prior to the

RPGD that, as has been said, has not modified the concepts of responsible and

treatment manager.

The assumptions of data processing for advertising purposes and within the framework of a

contract for the provision of services in accordance with the LCSP, analyzed in the STS

772/2020 and in the legal report of the AEPD dated 11/20/2019, with reference

internal 0007/2019, respectively, so repeated in the pleadings brief of the

MAEC, are cited in the resolution proposal and in this act as examples of

processing carried out on behalf of the data controller without this

entity accesses the data used or the use of personal databases of

third parties.

III

The rights of individuals regarding the protection of personal data are

regulated in articles 15 to 22 of the RGPD and 13 to 18 of the LOPDGDD. I know

contemplate the rights of access, rectification, deletion, opposition, right to

limitation of treatment and right to portability.

The formal aspects related to the exercise of these rights are established in the

articles 12 of the RGPD and 12 of the LOPDGDD.

Article 12 “Transparency of information, communication and modalities of

exercise of rights” of the RGPD establishes the following:

"1. The person responsible for the treatment will take the appropriate measures to facilitate the interested party

all information indicated in articles 13 and 14, as well as any communication with

in accordance with articles 15 to 22 and 34 regarding the treatment, in a concise, transparent,

intelligible and easily accessible, in clear and simple language, in particular any information

specifically targeted at a child. The information will be provided in writing or by other

means, including, if applicable, by electronic means. When requested by the interested party, the

Information may be provided verbally as long as the identity of the interested party is proven.

By other means.

2. The person responsible for the treatment will facilitate the interested party in the exercise of their rights under

of articles 15 to 22. In the cases referred to in article 11, paragraph 2, the person responsible

will not refuse to act at the request of the data subject in order to exercise their rights under

Articles 15 to 22, unless you can show that you are unable to identify the

interested.

3. The data controller will provide the interested party with information regarding their actions

on the basis of a request under articles 15 to 22, and, in any case, in the

period of one month from receipt of the request. This period may be extended for another

two months if necessary, taking into account the complexity and number of requests. The

responsible will inform the interested party of any of said extensions within a month to

from receipt of the request, indicating the reasons for the delay. When the interested

submit the application electronically, the information will be provided electronically.

electronic when possible, unless the interested party requests that it be provided in another way.

mode."

4. If the person in charge of the treatment does not process the request of the interested party, he will inform him without

delay, and no later than one month after receipt of the request, of the reasons for

its non-action and the possibility of presenting a claim before a control authority

and to exercise legal actions.

5. The information provided under articles 13 and 14 as well as all communication and

any action carried out under articles 15 to 22 and 34 will be free of charge.

When the requests are manifestly unfounded or excessive, especially due to

its repetitive nature, the data controller may: a) charge a reasonable fee in

depending on the administrative costs incurred to facilitate the information or communication

or perform the requested action, or b) refuse to act on the request. The responsible

of the treatment will bear the burden of demonstrating the manifestly unfounded or

excessive request.

6. Without prejudice to the provisions of article 11, when the data controller has

reasonable doubts in relation to the identity of the natural person who makes the request to which

referred to in articles 15 to 21, you may request that additional information be provided

necessary to confirm the identity of the interested party.

7. The information that must be provided to the interested parties under articles 13 and 14

may be transmitted in combination with standardized icons that allow the provision of

easily visible, intelligible and clearly legible form an adequate overview of the

planned treatment. The icons that are presented in electronic format will be legible

mechanically.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92

in order to specify the information to be presented through icons and the

procedures for providing standardized icons".

For its part, article 12 "General provisions on the exercise of rights"

of the LOPDGDD, in sections 2, 3 and 4, adds the following:

"two. The person responsible for the treatment will be obliged to inform the affected party about the means at its disposal.

disposition to exercise the corresponding rights. Media should be easily

accessible to the affected. The exercise of the right may not be denied for the sole reason

to choose the affected by another means.

3. The person in charge may process, on behalf of the person in charge, the requests for exercise

formulated by those affected by their rights if this is established in the contract or legal act

that link them.

4. Proof of compliance with the duty to respond to the request to exercise their rights.

rights formulated by the affected party will fall on the person responsible".

When data processing is carried out on behalf of a data controller

treatment, in accordance with the provisions of article 28 of the RGPD, the

in charge of the treatment "will assist the person in charge… so that he can comply with

its obligation to respond to requests that have as its object the exercise of the

rights of the interested parties established in Chapter III". This obligation must

be stipulated in the contract or legal act that binds the person in charge with respect to the

responsible (section 3 of the aforementioned article 28 of the RGPD).

In accordance with the provisions of these rules, the data controller

must arbitrate formulas and mechanisms to facilitate the interested party in the exercise of their

rights, which will be free (without prejudice to the provisions of articles 12.5 and 15.3

of the GDPR); and must give instructions to the person in charge of the treatment, if any,

to send you the requests you receive or to process them conveniently,

if so provided in the contract or legal act that binds them. Also, the

responsible for the treatment or the person in charge, where appropriate, are obliged to respond

requests made no later than one month, unless they can show that

they are not in a position to identify the interested party; as well as to express their reasons

in case they do not respond to the request.

From the foregoing, it follows that the request for the exercise of rights made by the

The interested party must be answered in any case, falling on the person in charge

proof of compliance with this duty.

This obligation to act is not enforceable when the data controller

can demonstrate that it is not in a position to identify the interested party (in cases

referred to in article 11.2 of the RGPD). In cases other than those provided for in this

article, in which the data controller has reasonable doubts in relation to

with the identity of the applicant, may require additional information necessary to

confirm that identity.

In this regard, Recital 64 of the RGPD is expressed in the following terms:

“(64) The controller must use all reasonable measures to verify the

identity of data subjects requesting access, in particular in the context of services

online and online identifiers. The person in charge must not keep personal data with

the sole purpose of being able to respond to possible requests”.

Regarding the right of opposition, the RGPD stipulates in its article 21 what

Next:

"1. The interested party shall have the right to object at any time, for reasons related to

with your particular situation, to which personal data that concerns you are subject to a

treatment based on the provisions of article 6, paragraph 1, letters e) or f), including the

profiling on the basis of those provisions. The data controller

will stop processing personal data, unless it proves compelling legitimate reasons for the processing.

treatment that prevail over the interests, rights and freedoms of the interested party, or

for the formulation, exercise or defense of claims.

2. When the processing of personal data is for the purpose of direct marketing, the

The interested party will have the right to oppose the processing of personal data at any time.

concerning you, including profiling to the extent that it is related to

said marketing.

3. When the interested party opposes the treatment for direct marketing purposes, the data

data will no longer be processed for said purposes.

4. At the latest at the time of the first communication with the data subject, the right

indicated in sections 1 and 2 will be explicitly mentioned to the interested party and will be

presented clearly and apart from any other information.

5. In the context of the use of information society services, and notwithstanding

provided for in Directive 2002/58/EC, the interested party may exercise their right to object by

automated means that apply technical specifications.

6. When personal data is processed for scientific or historical research purposes or for

statistics in accordance with article 89, paragraph 1, the interested party shall have the right, by

reasons related to your particular situation, to oppose the processing of personal data

that concern him, unless it is necessary for the fulfillment of a mission carried out by

reasons of public interest".

The owner of the personal data may exercise before the

responsible for the treatment a series of rights, among which is the right to

opposition to treatment.

In this case, there is evidence that the claimant formally addressed the MAEC stating

your opposition to the use of your personal data within the framework of the program

"***PROGRAMA.1", without the claimed entity responding to the exercise of the

law. Not even the MAEC, as data controller, has provided the

mechanisms and procedures necessary to address the exercise of rights by

citizens, even going so far as to affirm that this obligation corresponds to the

carriers that serve you.

Obviously, being the MAEC the entity responsible for the treatment, the right

exercised by the claimant on two occasions cannot be understood as addressed, as

said entity intends, with the response by which the claimant is informed that in order to

To satisfy your claim, you must go to the telephone operators. It is given

circumstance, on the other hand, that the two requests to exercise rights

made by the claimant were not addressed by the MAEC and the response to which

this entity refers to is provided during the processing of transfer of the claim

carried out by this Agency in accordance with the provisions of article 65.4 of the

LOPDGDD.

Consequently, in accordance with the exposed evidence, the aforementioned facts

represent a violation of the provisions of article 21 of the RGPD, which gives rise to the

application of the corrective powers that article 58 of the aforementioned Regulation grants to

the Spanish Data Protection Agency.

Failure to comply with the indicated precept is typified as an infraction in the

section 5.b) of article 83 of the RGPD, which under the heading “General conditions

for the imposition of administrative fines” provides the following:

“Infractions of the following provisions will be sanctioned, in accordance with section

2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a company,

of an amount equivalent to a maximum of 4% of the total annual global turnover of the

previous financial year, opting for the highest amount:

(…)

b) the rights of the interested parties according to articles 12 to 22".

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

infractions the acts and behaviors referred to in sections 4, 5 and 6 of the

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

present organic law".

For the purposes of the limitation period, the LOPDGDD in its article 72, "Infringements

considered very serious", states the following:

"1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679,

considered very serious and will prescribe after three years the infractions that suppose a

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

(…)

k) The impediment or the hindrance or the repeated non-attention of the exercise of the rights

established in articles 15 to 22 of Regulation (EU) 2016/679".

On this issue, Supreme Court Judgment 772/2020, of June 15,

declares the following:

"The sanctioned conduct of obstruction or impediment by XXX of the exercise by your client

of the right to oppose the processing of your data, it is stated that said company does not

adopted any kind of measure or precaution to avoid sending advertising to the

email addresses of your client by those companies to which

commissioned the realization of advertising campaigns.

The adoption of the necessary measures or precautions to ensure the effectiveness of the right to

opposition to the processing of your data by XXX, as responsible for the file,

subsist even if the advertising campaigns are not carried out using the data of their own

files, but with databases of other companies contracted by XXX, and in this case

It was proven that the appellant did not notify the companies with which it contracted the

realization of advertising services the opposition of the complainant to receive advertising from XXX,

nor in the end did he take any provision to ensure the exclusion of his client from the shipments

advertisers contracted with third parties".

IV

Secondly, the claimed entity is charged with the violation of article 28 of the

RGPD, "In charge of the treatment". In section 3, this precept establishes:

"3. The treatment by the person in charge will be governed by a contract or other legal act in accordance with the

Law of the Union or of the Member States, which binds the person in charge with respect to the

responsible and establishes the object, duration, nature and purpose of the treatment, the

type of personal data and categories of interested parties, and the obligations and rights of the

responsible. Said contract or legal act shall stipulate, in particular, that the person in charge:

a) will process personal data only following documented instructions of the

responsible, including with respect to transfers of personal data to a third country or

an international organisation, unless required to do so under Union law

or of the Member States that applies to the person in charge; in such a case, the person in charge will inform the

responsible for that legal requirement prior to treatment, unless such Law prohibits it by

important reasons of public interest;

b) will guarantee that the persons authorized to process personal data have

committed to respecting confidentiality or are subject to an obligation of

confidentiality of a statutory nature;

c) take all necessary measures in accordance with article 32;

d) will respect the conditions indicated in sections 2 and 4 to resort to another person in charge of the treatment;

e) will assist the person in charge, taking into account the nature of the treatment, through measures appropriate technical and organizational measures, whenever possible, so that it can comply with their obligation to respond to requests that have as their object the exercise of rights of the interested parties established in chapter III;

f) will help the person in charge to guarantee the fulfillment of the obligations established in the articles 32 to 36, taking into account the nature of the treatment and the information to disposal of the manager;

g) at the choice of the person in charge, will delete or return all personal data once ends the provision of treatment services, and will delete existing copies unless that the conservation of personal data is required by virtue of the Law of the Union or of the member states;

h) will make available to the person in charge all the information necessary to demonstrate the compliance with the obligations established in this article, as well as to allow and contribute to the performance of audits, including inspections, by the person in charge or another auditor authorized by said person in charge.

In relation to the provisions of letter h) of the first paragraph, the person in charge will inform immediately to the controller if, in his opinion, an instruction violates this Regulation or other provisions on data protection of the Union or of the Member states".

These specific obligations may be supervised by the authorities of data protection, without prejudice to the control that may be carried out in relation to with compliance with the Regulation or the LOPDGDD by the person responsible for the

treatment.

In accordance with the provisions of article 28 RGPD, the person in charge and the person in charge

of data processing must regulate the processing of data in a contract or act

legal that binds the person in charge with respect to the person in charge; that contract or legal act

must establish the object, duration, nature and purpose of the treatment, the

type of personal data and categories of interested parties, the obligations and rights of the

responsible etc

In this case, there is no evidence that the MAEC entity and the telephone operators

responsible for transferring to citizens who travel abroad the information

arranged within the framework of the program "***PROGRAMA.1" had formalized any

contract or legal act that regulates the use of the personal data of those

citizens by the operators, contrary to the provisions of the aforementioned article

28.3 of the GDPR.

The need to formalize the performance of processing on behalf of third parties

by means of a writing, or in any way that allows to prove its celebration and

content, was already regulated in the Organic Law 15/1999, of December 13, of

Protection of Personal Data (LOPD). Therefore, the breach of

this obligation on the part of the MAEC is not justified by the fact that the initiative

“***PROGRAMA.1” had been arranged prior to the application of the RGPD or

of the LRJSP, contrary to what was indicated by said entity in its allegations. Either

This circumstance exempts the respondent from the obligation to adapt their actions to the

cited norms, once they were fully applicable.

Consequently, in accordance with the exposed evidence, the aforementioned facts represent a violation of the provisions of article 28.3 of the RGPD, typified as infringement in section 4.a) of article 83 of the RGPD, which under the rubric "General conditions for the imposition of administrative fines", which establishes the Next:

"4. Violations of the following provisions will be sanctioned, in accordance with the section 2, with administrative fines of a maximum of EUR 10,000,000 or, in the case of a company, of an amount equivalent to a maximum of 2% of the total annual turnover of the previous financial year, opting for the highest amount:

a) the obligations of the person in charge and the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43;".

For the purposes of the limitation period, the LOPDGDD in its article 73 k), "Infringements considered serious", states the following:

"Based on the provisions of article 83.4 of Regulation (EU) 2016/679, they 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:

k) Entrust data processing to a third party without the prior formalization of a contract or another written legal act with the content required by article 28.3 of the Regulation (EU) 2016/679".

v

Once verified that the entity carried out the typical actions -infringement of the established in articles 21 and 28.3 of the RGPD-, we must analyze if the subjective element of guilt.

The presence of the subjective element is essential to demand in the field of Law Administrative Sanctioning responsibility for the illicit committed, since it does not fit in

this framework impose sanctions based on the strict liability of the alleged offender. Thus, in STC 76/1999 the High Court affirms that the sanctions administrative ones participate in the same nature as criminal ones, being one of the manifestations of the ius puniendi of the State, and that, as a requirement derived from the principles of legal certainty and criminal legality enshrined in articles 9.3 and 25.1 of the CE, the presence of the element of guilt is essential as condition for the creation of sanctioning responsibility.

The principle of culpability is required in the sanctioning procedure and thus the STC 246/1991 considers inadmissible in the field of sanctioning administrative law a liability without fault. But the principle of fault does not imply that it can only punish an intentional action and in this regard article 28 of the Law 40/2015 of the Legal Regime of the Public Sector, under the heading "Responsibility", provides the following:

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

The facts set forth in the preceding Basis show that the claimed did not act with the diligence to which it was obliged. In this case, it turns out It is obvious that the program “***PROGRAMA.1” entails carrying out activities of

personal data processing. Even so, the MAEC entity ordered its execution without

enable adequate mechanisms and procedures to attend to the rights of

interested parties and entrusted third parties with sending the messages that

constitute the main object of the program without adopting the specific formalities

imposed by the applicable regulations.

This action of the MAEC, which materializes in the infractions of which

blames the aforementioned entity, suffers from a serious lack of diligence.

The Supreme Court (STS April 16, 1991 and STS April 22, 1991) considers

that from the culpability element it follows “that the action or omission, qualified as

infraction punishable administratively, must be, in any case, attributable to its

author, by intent or recklessness, negligence or inexcusable ignorance. The same

The Court reasons that "it is not enough... to exculpate the behavior

typically unlawful the invocation of the absence of fault" but it is necessary

“that the diligence that was required by the person who alleges its non-existence has been used”

(STS January 23, 1998).

Also connected with the degree of diligence that the data controller is

obliged to deploy in the fulfillment of the obligations imposed by the

data protection regulations can be cited the SAN of 10/17/2007 (Rec. 63/2006),

which specified: “(...) the Supreme Court has been understanding that there is imprudence

whenever a legal duty of care is disregarded, that is, when the offender fails to

behaves with due diligence."

Furthermore, the National Court in matters of data protection of

personal character, has declared that "simple negligence or breach of

the duties that the Law imposes on the persons responsible for files or the

data processing to exercise extreme diligence...” (SAN June 29, 2001).

It is concluded, therefore, contrary to what was objected by the MAEC entity, that the element

subjective is present in the two imputed infractions.

SAW

On the other hand, article 83.7 of the RGPD provides that, without prejudice to the

corrective powers of the control authorities under art. 58, paragraph 2,

each Member State may lay down rules on whether and to what extent

impose administrative fines on authorities and public bodies established in

that Member State.

The LOPDGDD in its article 77, “Regime applicable to certain categories of

responsible or in charge of the treatment”, establishes the following:

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

are responsible or in charge:

a) The constitutional bodies or those with constitutional relevance and the institutions of the

autonomous communities analogous to them.

b) The jurisdictional bodies.

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

and the entities that make up the Local Administration.

d) Public bodies and public law entities linked to or dependent on the

Public administrations.

e) The independent administrative authorities.

f) The Bank of Spain.

g) Public law corporations when the purposes of the treatment are related

with the exercise of powers of public law.

h) Public sector foundations.

I) Public Universities.

j) The consortiums.

k) The parliamentary groups of the Cortes Generales and the Legislative Assemblies

autonomous, as well as the political groups of the Local Corporations.

2. When those responsible or in charge listed in section 1 commit any of the

the infractions referred to in articles 72 to 74 of this organic law, the authority of

protection of data that is competent will issue a resolution sanctioning them with

warning. The resolution will also establish the measures to be adopted so that

stop the behavior or correct 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 which

depends hierarchically, where appropriate, and those affected who had the status of

interested, if any.

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

It will also propose the initiation of disciplinary actions when there are indications

enough for it. In this case, the procedure and the sanctions to be applied will be the

established in the legislation on the disciplinary or sanctioning regime resulting from

app.

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

existence of technical reports or recommendations for treatment that had not been

duly attended to, the resolution in which the sanction is imposed will include a

reprimand with the name of the responsible position and the publication will be ordered in the

Official Gazette of the corresponding State or Autonomous Community.

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

in relation to the measures and actions referred to in the preceding sections.

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

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

this article.

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

It will be, in terms of the publicity of these resolutions, to what its regulations have

specific".

Thus, considering the possibility contemplated in this precept to correct the

actions of those responsible that do not comply with the regulations for the protection of

personal data, when those responsible listed in section 1 committed

any of the infractions referred to in articles 72 to 74 of the aforementioned Law

Organic, in this case it is appropriate to impose on the claimed entity, that is, on the entity

MAEC, a warning sanction.

Likewise, it is contemplated that the resolution issued may establish the measures

that it is appropriate to adopt so that the conduct ceases, the effects of the infraction are corrected

that had been committed and the necessary adaptation is carried out, in this case, to

the requirements contemplated in articles 21 and 28.3 of the RGPD, as well as the

provision of means accrediting compliance with the requirements.

Thus, in accordance with the provisions of the aforementioned article 77 of the LOPDGDD, it is appropriate require the responsible entity so that, within the term indicated in the operative part, adapt its actions to the personal data protection regulations, with the scope expressed in the previous Foundations of Law. Specifically, you must set the mechanisms and management processes necessary to enable the attention of the rights recognized to the interested parties and formalize, in accordance with the provisions of the article 28.3 of the RGPD, the relationship that binds the MAEC and the operators of telephony within the framework of the "***PROGRAMA.1" program. Also, you must attend to the right exercised by the claimant and communicate to the telephone operators the decision adopted in this regard so that they stop sending said claimant SMS messages within the framework of the program "***PROGRAMA.1".

In this regard, it is noted that not meeting the requirements of this body can be considered as a serious administrative infraction by "not cooperating with the Control Authority" before the requirements made, being able to be valued such conduct at the time of opening an administrative sanctioning procedure.

Therefore, in accordance with the applicable legislation and having assessed the criteria for graduation of sanctions whose existence has been proven, the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE on the entity MINISTRIES OF FOREIGN AFFAIRS, EUROPEAN UNION AND COOPERATION, with CIF ***CIF.1, for the infraction of the articles 21 and 28.3 of the RGPD, typified, respectively, in articles 83.5.b) and

83.4.a) of the same Regulation, and classified as very serious and serious for the purposes of prescription in articles 72.1.k) and 73.k) of the LOPDGDD, a sanction of warning.

SECOND: TO REQUEST the entity MINISTRIES OF FOREIGN AFFAIRS, EUROPEAN UNION AND COOPERATION, so that, within three months, as soon as from the notification of this resolution, adapt its actions to the regulations of protection of personal data, with the scope expressed in the Foundation of Right V, and justify before this Spanish Data Protection Agency the attention of this requirement. The text of the resolution establishes which have been the infractions committed and the facts that have given rise to the violation of the data protection regulations, from which it is clearly inferred what are the measures to be adopted, without prejudice to the type of procedures, mechanisms or specific instruments to implement them correspond to the sanctioned party, since is the data controller who fully knows your organization and must decide, based on proactive responsibility and risk approach, how to comply with the RGPD and the LOPDGDD.

THIRD: NOTIFY this resolution to the entity MINISTRIES OF FOREIGN AFFAIRS, EUROPEAN UNION AND COOPERATION.

FOURTH:

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

COMMUNICATE this resolution to the Ombudsman,

In accordance with the provisions of article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the Interested parties may optionally file an appeal for reconsideration before the

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

counting from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

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

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

aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP,

may provisionally suspend the firm resolution in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact by

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

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

web/], or through any of the other registers provided for in art. 16.4 of the

aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the

documentation proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of two months from the day following the

notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-26102021

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es