 File No.: EXP202200399

RESOLUTION OF TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTEER

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

to the following

BACKGROUND

FIRST: On July 18, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against BAYARD REVISTAS,

S.A. (hereinafter, the claimed party), through the Agreement that is transcribed:

<<

File No.: EXP202200399

AGREEMENT TO START A SANCTION PROCEDURE

Of the actions carried out by the Spanish Agency for Data Protection

(AEPD) and based on the following:

FACTS

FIRST: D.A.A.A. (hereinafter, the complaining party) dated November 27,

2021 filed a claim with the Spanish Data Protection Agency. The

claim is directed against BAYARD REVISTAS, S.A with NIF A78874054 (in

forward, BAYARD). The grounds on which the claim is based are as follows:

The complaining party informs this Agency that he has received an email

by the person in charge of the web portal ***URL.1, in which he was informed about the

unauthorized access to the database by an unauthorized third party,

being responsible BAYARD.

According to the email, location and contact data of the

people who had provided their information on the website through the form of

Registration.

The person in charge assures that he has solved all the vulnerabilities that have

enabled the attack, has implemented the protocols to follow in the event of an incident

related to data protection, and has adopted a series of measures, including

which is the encryption of stored information.

Attached to this claim is the screenshot of the email received

on November 19, 2021, warning of the breach.

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

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

hereinafter LOPDGDD), said claim was transferred to BAYARD, so that

proceed to its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements set forth in the regulations of

Data Protection.

The transfer was sent on January 21, 2022 by electronic notification,

in accordance with article 41 of Law 39/2015, of October 1, on the Procedure

Common Administrative of Public Administrations (LPACAP).

This notification was automatically rejected after ten days had elapsed

natural from its availability for access according to paragraph 2, article

43, of Law 39/2015, of October 1, of the Common Administrative Procedure of the

Public administrations; reiterating the transfer by certified mail, dated 01

of February 2022, resulting in the latter with an "unknown" status without the possibility of

locate the person in charge.

THIRD: On February 23, 2022, in accordance with article 65 of the

LOPDGDD, the claim filed by the claimant was admitted for processing.

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

of previous investigative actions to clarify the facts in

matter, by virtue of the investigative powers granted to the authorities of

control in article 57.1 of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter RGPD), and in accordance with the provisions of the

Title VII, Chapter I, Second Section, of the LOPDGDD, dated March 1,

2022 BAYARD information was required, in order to clarify the aspects

related to the security breach giving rise to the claim filed.

The request for information was sent by electronic notification, in accordance with

to article 41 of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (LPACAP).

Although this notification was automatically rejected after ten

calendar days from its availability for access according to paragraph 2,

Article 43 of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations; reiterating the transfer by mail

certified, dated March 14, 2022, but using a different fiscal address

to the one used in the transfer, address obtained from the website of the person in charge, resulting

this last successful request with an acknowledgment date of March 22, 2022.

FIFTH: On April 6, 2022, a response to said request for information is received.

SIXTH: Within the framework of the aforementioned preliminary investigation actions,

again, request for information dated April 25 of that same year.

The request for information was sent by electronic notification, in accordance with to article 41 of Law 39/2015, of October 1, on Administrative Procedure Common Public Administrations (LPACAP).

SEVENTH: On May 5 of that same year, said request was answered. of information.

EIGHTH: Of the previous investigation actions carried out for the clarification of the facts in question, there has been knowledge of the following ends:

In relation to the person responsible for processing the personal data processed by the web portal ***URL.1 as well as the possible existence of a delegate of data protection (DPD), by BAYARD it is answered:

~ The controller of this portal is BAYARD REVISTAS S.A.

~ The DPD is GRUPO ADAPTALIA LEGAL FORMATIVO S.L, however, in the At the time of the security breach, there was only one consulting contract on data protection, and that this contract is extended on January 17, 2022 by which these extended services for the previous group to act as a delegate for the protection of data of the person in charge BAYARD REVISTAS S.A. This link is also communicated to this Agency on March 3, 2022, through the Subdirectorate General for Promotion and Authorizations, we are provided with a copy of the registration document.

Regarding the type of affected data and chronological description of the

events that occurred, BAYARD replies:

That on October 22, 2021, an email signed by an external person is received, which is

identified as a supposed researcher and disseminator specialized in cybersecurity

web, reporting that he had managed to access the company's data as a result of

a vulnerability of the website, providing as proof a screenshot with the

names of the database tables, without providing evidence about the leak of

data.

That this attack had not been carried out for malicious purposes but with the intention of

ethical hacking, therefore of the vulnerability notice to the person in charge of the web without

no criminal purpose.

That the filtered data correspond to identification data, contact data,

Approximate location and in some cases identification data of children under the age of

age.

That from this moment the services of a third company were contracted

expert in cybersecurity (ACUNETIX) to identify and correct the

web vulnerabilities.

That the number of affected would correspond to the total number of users of the portal

web, around this number 464762.

That no user has communicated that their data could have been used.

Regarding the risk analysis and the security measures that were

implanted prior to the incident, BAYARD answers that they did have analysis of

risks previously carried out through the AEPD MANAGES tool,

providing an annex as evidence of this.

However, after analyzing it, it is concluded that this document refers to the

report generated by the EIPD MANAGEMENT tool of this Agency and is

includes both a description of the data life cycle and a relationship of

regulatory compliance requirements aimed at risk management, but not

identify or analyze other risk factors with different origins of non-compliance

normative, for example, those related to the technology used.

The security measures implemented prior to the breach, and which had been

shown to be inefficient, were:

- (…)

Regarding the containment measures, the following are indicated:

- Hire cybersecurity services to identify all the vulnerabilities that

allowed the filtration and apply reinforcement measures to protect the SQL DBs from the

company.

- Communicate the breach to GRUPO ADAPTALIA LEGAL FORMATIVO S.L, provider

external specialized in data protection (which at that time provided services

advice on data protection, to analyze and determine the needs and

obligations regarding notification and communication to both the AEPD and those affected.

- Refresh and implement internally the action protocol in case of

security breach so that all staff know what to do in the event of a breach.

awareness of security breach.

- Communicate with those affected.

- Notify the AEPD.

Regarding the communication to those affected, BAYARD responds that:

It was communicated via email to the nearly 470,000 affected, on November 20

2021, providing a copy of the email sent to one of those affected.

After analyzing it, it is determined that this email was sent on November 19,

2021 to one of the affected assumptions, transferring information on:

o The type of data affected, communicating that it is personal data.

contact and location provided through the registration form of the

website.

o The circumstances in which the events occurred, reporting on the

email received by the alleged hacker.

o The possible consequences, such as loss of confidentiality of the

information provided through the web portal.

o The corrective measures adopted and that correspond to those mentioned

previously.

Regarding the notification of the gap before this Agency, BAYARD answers that

immediately after analyzing the gap by GRUPO ADAPTALIA, we proceed to

notify the same before this Agency, providing as proof a copy of the registry of

notification input.

From the analysis of this we can extract the following information:

- That it is detected on October 22, 2021 by the notification of an external third party and that

It is considered resolved on October 26, 2021.

It is reported by an external person who has been able to have access to the data by sending

as evidence only a screenshot with the name of the tables of the

database, without providing the data.

- That the data affected are basic, location and contact data.

- They indicate that among the affected people there is data identifying minors.

- That the incident log has been updated.

- That among the new security measures is the performance of audits

periodic and data encryption.

In relation to the existence of third party companies that could act as

those in charge of processing personal information, respond that the only third party

is Amazon Web Services (AWS) with whom they have contracted the web hosting,

signing the general contracting conditions regarding the protection of

data published by AWS at ***URL.2

FOUNDATIONS OF LAW

Yo

Competition

By virtue of the powers that article 58.2 of Regulation (EU) 2016/679 of the

European Parliament and of the Council of April 27, 2016 on the protection of

individuals with regard to the processing of personal data and the free

circulation of these data (RGPD) recognizes each control authority, and according to what

established in articles 47 and 48 of the LOPDGDD, the Director of the Agency

Spanish Data Protection is competent to initiate and resolve this

process.

II

Previous questions

In the present case, in accordance with the provisions of article 4.1 of the RGPD, it consists

carrying out personal data processing, since BAYARD, among

other treatments, performs the collection, registration, conservation ... etc, of the data of

contact and location provided by users, through the form of

website registration.

BAYARD carries out this activity in its capacity as data controller, given

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

GDPR.

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

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

those breaches of security that cause the destruction, loss or alteration

accidental or illicit of personal data transmitted, conserved or processed in another

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

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

circumstances indicated above, categorized as a breach of confidentiality when

having accessed the data of the users of the web portal, due to a vulnerability of the

website.

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

imposition of a sanction directly by this Agency, since it is necessary

analyze the diligence of those responsible and in charge and the security measures

applied.

Within the principles of treatment provided for in article 5 of the RGPD, the

integrity and confidentiality of personal data is guaranteed in section 1.f)

of article 5 of the RGPD. For its part, the security of personal data comes

regulated in articles 32, 33 and 34 of the RGPD, which regulate the security of the

treatment, notification of a violation of the security of personal data to

the control authority, as well as the communication to the interested party, respectively.

III

Article 5.1.f) of the RGPD

Article 5.1.f) “Principles related to treatment” of the RGPD establishes:

"1. The personal data will be:

(…)

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

personal data, including protection against unauthorized processing or

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

of appropriate technical or organizational measures ("integrity and

confidentiality”).”

In the present case, it is stated that the personal data of those affected, contained in the

BAYARD's database, were improperly exposed to a third party.

On October 22, 2021, BAYARD receives an email signed by an external person, who

identified himself as a supposed researcher and disseminator specializing in

web cybersecurity, reporting that he had managed to access the data of the

company as a result of a website vulnerability, providing as evidence capture

screen with the names of the database tables and without providing proof

about data breach.

In accordance with the evidence available in this agreement of

initiation of the sanctioning procedure, and without prejudice to what results from the

instruction, it is considered that the known facts could constitute a

infringement, attributable to BAYARD, for violation of article 5.1.f) of the RGPD.

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

IV

If confirmed, the aforementioned infringement of article 5.1.f) of the RGPD could lead to the

commission of the offenses typified in article 83.5 of the RGPD that under the

The heading "General conditions for the imposition of administrative fines" provides:

“The infractions of the following dispositions 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 this regard, the LOPDGDD, in its article 71 "Infringements" establishes that

“The acts and behaviors referred to in sections 4,

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

contrary to this organic law.

For the purposes of the limitation period, article 72 “Infringements considered very

serious” of the LOPDGDD indicates:

"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:

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

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

Sanction for the infringement of article 5.1.f) of the RGPD

v

For the purposes of deciding on the imposition of an administrative fine and its amount,

accordance with the evidence available at the present time.

agreement to initiate sanctioning proceedings, and without prejudice to what results from the

investigation, the infringement in question is considered to be serious for the purposes of

RGPD and that it is appropriate to graduate the sanction to be imposed in accordance with the following

criteria established by article 83.2 of the RGPD:

As aggravating factors:

-

g) the categories of personal data affected by the infringement.

In the present case, the filtered data corresponds to identifying data, of

contact, approximate location data and in some cases data

identification of minor children.

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established in section 2 of article 76 "Sanctions and measures

corrective measures" of the LOPDGDD:

As aggravating factors:

-

b) The link between the activity of the offender and the performance of treatments

of personal data.

BAYARD collaborates with its publications in the dissemination of culture and

promotion of reading, having a database of users of the

website.

-

f) Affectation of the rights of minors.

As stated in the file, the filtered data corresponds to data

identifying, contact, approximate location data and in some

cases identifying data of minor children.

The balance of the circumstances contemplated in article 83.2 of the RGPD and the

Article 76.2 of the LOPDGDD, with respect to the infraction committed by violating the

established in article 5.1.f) of the RGPD, allows initially setting a penalty of

AMOUNT OF €30,000 (thirty thousand euros).

SAW

Article 32 of the GDPR

Article 32 “Security of treatment” of the RGPD establishes:

"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 guarantee the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

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

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and evaluation of the effectiveness

technical and organizational measures to guarantee the security of the

treatment.

2. When evaluating the adequacy of the security level, particular account shall be taken of

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

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

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

unauthorized access to said data.

3. Adherence to an approved code of conduct under article 40 or to a

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present article.

4. The person in charge and the person in charge of the treatment will take measures to guarantee that

any person acting under the authority of the person in charge or the person in charge and

has access to personal data can only process said data following

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

the Union or the Member States.

In the present case, BAYARD, as the data controller, is

obliged to apply the appropriate technical and organizational measures to guarantee a

level of security appropriate to the risk presented by the data processing.

"(...)".

Although the risk analysis they provide is the output report generated by the

MANAGE EIDP tool of this Agency.

This tool serves only as a guide to establish the basic elements

that must be taken into account in the risk analysis of treatments and

impact assessments, however, is not valid to identify

exhaustively the possible risk factors that must be evaluated to protect the

rights and freedoms of the interested parties present in the data processing.

The risk analysis provided lacks the identification of factors that make

reference to possible threats of web attacks related to the loss of

confidentiality, availability or integrity of the personal data processed through

of the portal itself ***URL.1.

Article 32 of the RGPD does not establish a list of security measures that are

of application according to the data that are object of treatment, but

establishes that the person in charge and the person in charge of the treatment will apply

technical and organizational that are appropriate to the risk involved in the treatment,

taking into account the state of the art, the application costs, the nature,

scope, context and purposes of the treatment, the risks of probability and severity

for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and proportionate to the

detected risk, pointing out that the determination of technical measures and

organizational measures must be carried out taking into account: pseudonymization and encryption,

capacity to guarantee confidentiality, integrity, availability and resilience, the

ability to restore availability and access to data after an incident, process

of verification (not audit), evaluation and assessment of the effectiveness of the

measures.

In relation to the preventive measures implemented prior to the breach, no

There is no link between these measures and the risk analysis carried out,

Therefore, it cannot be demonstrated that said measures were deployed to mitigate a

certain level of inherent risk of processing for the rights and freedoms of

the people whose personal data is processed.

It is noteworthy that with (…)".

(...).

And lastly, regarding the contingency measures, BAYARD in its writing of

answer literally says:

"(…)."

In accordance with the evidence available in this agreement of

initiation of the sanctioning procedure, and without prejudice to what results from the

instruction, it is considered that the known facts could constitute a

infringement, attributable to BAYARD, for violation of article 32 of the RGPD.

Classification of the infringement of article 32 of the RGPD

7th

If confirmed, the aforementioned violation of article 32 of the RGPD could lead to the

commission of the offenses typified in article 83.4 of the RGPD that under the

The heading "General conditions for the imposition of administrative fines" provides:

“The infractions of the following dispositions will be sanctioned, in accordance with the

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

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

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

the largest amount:

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

11, 25 to 39, 42 and 43; (…)”

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

“The acts and behaviors referred to in sections 4,

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

contrary to this organic law.

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

of the LOPDGDD indicates:

“Based on the provisions of article 83.4 of Regulation (EU) 2016/679,

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

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

following:

(…)

f) The lack of adoption of those technical and organizational measures that

are appropriate to guarantee an adequate level of security when

risk of treatment, in the terms required by article 32.1 of the

Regulation (EU) 2016/679.

Sanction for the infringement of article 32 of the RGPD

viii

For the purposes of deciding on the imposition of an administrative fine and its amount,

accordance with the evidence available at the present time.

agreement to initiate sanctioning proceedings, and without prejudice to what results from the

investigation, the infringement in question is considered to be serious for the purposes of

RGPD and that it is appropriate to graduate the sanction to be imposed in accordance with the following

criteria established by article 83.2 of the RGPD:

As aggravating factors:

-

g) the categories of personal data affected by the infringement.

In the present case, the filtered data corresponds to identifying data, of

contact, approximate location data and in some cases data

identification of minor children.

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established in section 2 of article 76 “Sanctions and measures

corrective measures” of the LOPDGDD:

As aggravating factors:

-

b) The link between the activity of the offender and the performance of treatments

of personal data.

BAYARD collaborates with its publications in the dissemination of culture and

promotion of reading, having a database of users of the

website.

-

f) Affectation of the rights of minors.

As stated in the file, the filtered data corresponds to data

identifying, contact, approximate location data and in some

cases identifying data of minor children.

The balance of the circumstances contemplated in article 83.2 of the RGPD and the

Article 76.2 of the LOPDGDD, with respect to the infraction committed by violating the

established in article 32 of the RGPD, allows initially setting a penalty of

€20,000 (amount of twenty thousand euros).

IX

GDPR Article 33

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

the control authority” of the RGPD establishes:

"1. In case of violation of the security of personal data, the person in charge of the

treatment will notify the competent control authority in accordance with the

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

who was aware of it, unless it is unlikely that such violation

constitutes a risk to the rights and freedoms of individuals

physical. If the notification to the supervisory authority does not take place within the period of 72

hours, must be accompanied by an indication of the reasons for the delay.

2. The person in charge of the treatment will notify without undue delay the person in charge of the

treatment the violations of the security of the personal data of which it has

knowledge.

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

a) describe the nature of the data security breach

including, where possible, the categories and number

approximate number of stakeholders affected, and the categories and approximate number

of affected personal data records;

b) communicate the name and contact details of the data protection delegate

data or another point of contact where further information can be obtained;

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

personal information;

d) describe the measures adopted or proposed by the person responsible for the

processing to remedy the data security breach

including, if applicable, the measures taken to mitigate the

possible negative effects.

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

is not, the information will be provided gradually without undue delay.

5. The data controller will document any breach of data security.

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

corrective measures taken. Said documentation will allow the authority of

control to verify compliance with the provisions of this article."

In the present case, it is clear that BAYARD has evidence of having suffered a

security breach of personal data on October 28, 2021 and has not

reported to this Agency, to date on November 11 of that same year.

On October 28, there was already evidence of the existence of web vulnerabilities that

would have made possible the loss of confidentiality in personal data, and it is in that

moment when it is transferred to the data protection advisory company so that

You will be told how to act accordingly.

To assess the notification needs, they used the formula that appears in the

“Guide for the management and notification of security violations”: Risk = P

(Volume) x I (Type x Impact), using the following parameters:

o Volume = 4 (Over 100,000)

o Typology = 1 (Non-sensitive data)

o Impact = 8 (Public, accessible on the internet)

However, and taking into account that on October 28 there was already evidence of the

possible breach that would affect personal data, there is a temporary delay in relation to

with the notification of the gap to this Agency, since it takes place on November 11

of 2021.

The same happens with the communication to those affected, which is carried out on a date

approximately November 20, 2021.

For this reason, it was decided to make a new request for information to BAYARD on the date

April 24, 2022 to clarify the following issues:

- Reasons that would justify the delay in notifying the Agency.

- Reasons that would justify the delay in communication with those affected.

Regarding the delay in notifying the security breach to the Agency,

indicate that, at the time of knowledge of this, BAYARD could not guarantee that

said gap was real, and therefore was unaware of the existing risk to the rights

and freedoms of the interested parties.

Providing the following: "(...)."

Although, no evidence has been found of this notification made on December 2

nor of the aforementioned affirmation; consequently, they cannot be

admit such reasons for delay.

In accordance with the evidence available in this agreement of

initiation of the sanctioning procedure, and without prejudice to what results from the

instruction, it is considered that the known facts could constitute a

infringement, attributable to BAYARD, for violation of article 33 of the RGPD.

Classification of the infringement of article 33 of the RGPD

X

If confirmed, the aforementioned violation of article 33 of the RGPD could lead to the

commission of the offenses typified in article 83.4 of the RGPD that under the

The heading "General conditions for the imposition of administrative fines" provides:

“The infractions of the following dispositions will be sanctioned, in accordance with the

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

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

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

the largest amount:

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

11, 25 to 39, 42 and 43; (…)”

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

“The acts and behaviors referred to in sections 4,

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

contrary to this organic law.

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

of the LOPDGDD indicates:

“Based on the provisions of article 83.4 of Regulation (EU) 2016/679,

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

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

following:

(…)

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

data from a security breach of personal data in accordance

with the provisions of article 33 of Regulation (EU) 2016/679. (…)”

Sanction for the infringement of article 33 of the RGPD

eleventh

For the purposes of deciding on the imposition of an administrative fine and its amount,

accordance with the evidence available at the present time.

agreement to initiate sanctioning proceedings, and without prejudice to what results from the

investigation, the infringement in question is considered to be serious for the purposes of

RGPD and that it is appropriate to graduate the sanction to be imposed in accordance with the following

criteria established by article 83.2 of the RGPD:

As aggravating factors:

-

g) the categories of personal data affected by the infringement.

In the present case, the filtered data corresponds to identifying data, of

contact, approximate location data and in some cases data

identification of minor children.

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established in section 2 of article 76 “Sanctions and measures

corrective measures” of the LOPDGDD:

As aggravating factors:

-

b) The link between the activity of the offender and the performance of treatments

of personal data.

BAYARD collaborates with its publications in the dissemination of culture and

promotion of reading, having a database of users of the

website.

-

f) Affectation of the rights of minors.

As stated in the file, the filtered data corresponds to data

identifying, contact, approximate location data and in some

cases identifying data of minor children.

The balance of the circumstances contemplated in article 83.2 of the RGPD and the

Article 76.2 of the LOPDGDD, with respect to the infraction committed by violating the

established in article 33 of the RGPD, allows initially setting a penalty of 2,000

€ (two thousand euros).

XII

Imposition of measures

Among the corrective powers provided in article 58 "Powers" of the RGPD, in the

Section 2.d) establishes that each control authority may “order the

responsible or in charge of the treatment that the treatment operations are

comply with the provisions of this Regulation, where appropriate, in a

certain manner and within a specified period…”.

The Spanish Agency for Data Protection in the resolution that puts an end to the

This procedure may order the adoption of measures, as established

in article 58.2.d) of the RGPD and in accordance with what is derived from the instruction

of the procedure, if necessary, in addition to sanctioning with a fine.

Therefore, by the Director of the Spanish Data Protection Agency, SE

AGREE:

FIRST: START A SANCTION PROCEDURE against BAYARD REVISTAS, S.A.

with NIF A78874054, for the alleged infringement of article 5.1.f) of the RGPD, typified

in article 83.5 of the RGPD.

START A SANCTION PROCEDURE against BAYARD REVISTAS, S.A with NIF

A78874054, for the alleged infringement of article 32 of the RGPD, typified in the

article 83.4 of the RGPD.

START A SANCTION PROCEDURE against BAYARD REVISTAS, S.A with NIF

A78874054, for the alleged infringement of article 33 of the RGPD, typified in the

article 83.4 of the RGPD.

SECOND: THAT for the purposes provided in article 64.2 b) of Law 39/2015, of 1
of October, of the Common Administrative Procedure of the Public Administrations
(hereinafter, LPACAP), the sanction that may correspond, without prejudice to what
result of the instruction, would be:
THIRTY THOUSAND EUROS (€30,000), for the alleged infringement of article 5.1.f) of the
RGPD, typified in article 83.5 of the RGPD.
TWENTY THOUSAND EUROS (€20,000), for the alleged infringement of article 32 of the RGPD,
typified in article 83.4 of the RGPD.
TWO THOUSAND EUROS (€2,000), for the alleged infringement of article 33 of the RGPD,
typified in article 83.4 of the RGPD.
FOURTH: APPOINT B.B.B. and, as secretary, to C.C.C.,
indicating that any of them may be challenged, as the case may be, in accordance with
established in articles 23 and 24 of Law 40/2015, of October 1, on the Regime
Legal Department of the Public Sector (LRJSP).
FIFTH: INCORPORATE to the disciplinary file, for evidentiary purposes, the
claim filed by the claimant and its documentation, as well as the
documents obtained and generated by the Subdirectorate General for Inspection of
Data in the actions prior to the start of this sanctioning procedure.
SIXTH: NOTIFY this agreement to BAYARD REVISTAS, S.A with NIF
A78874054, granting him a hearing period of ten business days to formulate
the allegations and present the evidence it deems appropriate. In his writing of
allegations you must provide your NIF and the procedure number that appears in the
header of this document.
If within the stipulated period it does not make allegations to this initial agreement, the same
may be considered a resolution proposal, as established in article
64.2.f) of Law 39/2015, of October 1, of the Common Administrative Procedure of

Public Administrations (hereinafter, LPACAP).

Pursuant to article 85 of the LPACAP, a proceeding has been initiated

sanctioning party, if the offender acknowledges his responsibility, the

procedure with the imposition of the appropriate sanction.

In accordance with the provisions of article 85 of the LPACAP, you may recognize your

responsibility within the term granted for the formulation of allegations to the

this initiation agreement; which will entail a reduction of 20% of the

sanction to be imposed in this proceeding. With the application of this

reduction, the sanction would be established at FORTY-ONE THOUSAND EUROS

(€41,600), resolving the procedure with the imposition of this sanction.

Similarly, you may, at any time prior to the resolution of this

procedure, carry out the voluntary payment of the proposed sanction, which

will mean a reduction of 20% of its amount. With the application of this reduction,

the sanction would be established at FORTY-ONE THOUSAND EUROS (€41,600) and its

payment would imply the termination of the procedure.

The reduction for the voluntary payment of the penalty is cumulative with the corresponding

apply for the acknowledgment of responsibility, provided that this acknowledgment

is revealed within the period granted to formulate allegations to the

initiation of the procedure. The voluntary payment of the amount referred to in paragraph

above may be made at any time prior to resolution. In this case, yes

were it appropriate to apply both reductions, the amount of the penalty would be established

THIRTY-ONE THOUSAND TWO HUNDRED EUROS (€31,200).

In any case, the effectiveness of any of the aforementioned reductions will be

conditioned to the abandonment or renunciation of any action or resource in via

against the sanction imposed, as provided in article 85.3 of the

LPACAP.

In case you chose to proceed to the voluntary payment of any of the amounts

indicated above (FOURTY-ONE THOUSAND EUROS (€41,600) or THIRTY-ONE

ONE THOUSAND TWO HUNDRED EUROS (€31,200), you must make it effective by paying

in account number ES00 0000 0000 0000 0000 0000 opened in the name of the Agency

Spanish Department of Data Protection in the banking entity CAIXABANK, S.A., indicating

in the concept the reference number of the procedure that appears in the

heading of this document and the reason for the reduction of the amount to which

welcomes

Likewise, you must send the payment receipt to the SGID to continue with the

procedure in accordance with the amount entered.

The procedure will have a maximum duration of nine months from the

date of the start-up agreement or, where appropriate, of the draft start-up agreement.

Once this period has elapsed, it will expire and, consequently, the file of

actions, in accordance with the provisions of article 64.2 of the LOPDGDD.

Sea Spain Marti

Director of the Spanish Data Protection Agency

935-110422

>>

SECOND: On July 27, 2022, the claimed party has proceeded to pay

the sanction in the amount of 31,200 euros making use of the two reductions

provided for in the Start Agreement transcribed above, which implies the

acknowledgment of responsibility.

THIRD: The payment made, within the period granted to formulate allegations to

the opening of the procedure, entails the waiver of any action or resource in via

administrative action against the sanction and acknowledgment of responsibility in relation to

the facts referred to in the Initiation Agreement.

FOUNDATIONS OF LAW

Yo

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

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

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

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

guarantee of digital rights (hereinafter, LOPDGDD), is competent to

initiate and resolve this procedure the Director of the Spanish Protection Agency

of data.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures

processed by the Spanish Agency for Data Protection will be governed by the provisions

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

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures."

II

Article 85 of Law 39/2015, of October 1, on Administrative Procedure

Common to Public Administrations (hereinafter, LPACAP), under the rubric

"Termination in sanctioning procedures" provides the following:

"1. Started a sanctioning procedure, if the offender acknowledges his responsibility,

the procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction is solely pecuniary in nature or it is possible to impose a

pecuniary sanction and another of a non-pecuniary nature, but the

inadmissibility of the second, the voluntary payment by the alleged perpetrator, in

any time prior to the resolution, will imply the termination of the procedure,

except in relation to the replacement of the altered situation or the determination of the

compensation for damages caused by the commission of the infringement.

3. In both cases, when the sanction is solely pecuniary in nature, the

competent body to resolve the procedure will apply reductions of, at least,

20% of the amount of the proposed sanction, these being cumulative with each other.

The aforementioned reductions must be determined in the notification of initiation

of the procedure and its effectiveness will be conditioned to the withdrawal or resignation of

any administrative action or recourse against the sanction.

The reduction percentage provided for in this section may be increased

regulations."

According to what was stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: TO DECLARE the termination of procedure EXP202200399, of

in accordance with the provisions of article 85 of the LPACAP.

SECOND: NOTIFY this resolution to BAYARD REVISTAS, S.A.

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 as prescribed by

the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure

Common of the Public Administrations, the interested parties may file an appeal

contentious-administrative 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.

Sea Spain Marti

Director of the Spanish Data Protection Agency