File No.: EXP202102640

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 August 8, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against NTT DATA SPAIN,

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

<<

File No.: EXP202102640

AGREEMENT TO START A SANCTION PROCEDURE

Of the actions carried out by the Spanish Data Protection Agency and in

based on the following

FACTS

FIRST: The Spanish Data Protection Agency has been made aware of

certain facts that could violate data protection legislation,

as a result of notifications to the Technological Innovation Division of

this Agency of different breaches of personal data by various

controllers and processors of the insurance sector, relating to the

unauthorized publication of customer data of such organizations.

Summary of notifications

(…)

The documentation provided includes:

□

(…)

On September 7, 2021, the Director of the Spanish Agency for

Data Protection urged the General Subdirectorate for Data Inspection (SGID) to

initiate the preliminary investigation actions referred to in article 67 of the

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

guarantee of digital rights (hereinafter, LOPDGDD) to investigate EVERIS

SPAIN S.L. with NIF B82387770 (hereinafter, EVERIS) in relation to the following

facts:

The unauthorized publication of customer data from different organizations of the

insurance industry.

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

of previous investigative actions to clarify the facts in

question, by virtue of the functions assigned to the control authorities in the

article 57.1 and the powers granted in article 58.1 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, having knowledge of the following extremes:

Chronology of the events according to the reports provided:

□

(…)

Regarding the causes that made the breach possible.

(…)

Regarding the affected data

(…)

Regarding the security measures implemented

(…)

FOUNDATIONS OF LAW

Yo

Competition

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

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, whenever EVERIS performs, in- among other treatments, the collection, conservation, use and dissemination of the following personal data of insured natural persons, such as: identification data, data of the subscribed policies, bank details…etc.

EVERIS carries out this activity in its capacity as data processor, given that is the person who processes personal data on behalf of the data controller, by virtue of of the aforementioned article 4.8 of the RGPD.

EVERYS is a provider of technological infrastructure management services for REIAL AUTOMÒBIL CLUB DE CATALUNYA (hereinafter, RACC), a company provided- assistance services on behalf of GACM SEGUROS GENERALES, COMPA- ÑÍA DE SEGUROS Y REASEGUROS S.A.U. (GACM) as reinsurance entity of attendance.

Article 4 section 12 of the RGPD defines, in a broad way, the "violations of se- 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 cir- circumstances indicated above, categorized as a breach of confidentiality, by having published in different forums the sale of the users of a security company guros dedicated to the automobile sector, as well as records with personal information of Spanish clients of the insurance company ZURICH INSURANCE PLC SUCUR- SALT IN SPAIN.

It should be noted that receiving a complaint about a security breach

does not imply the imposition of a sanction directly, since it is necessary to analyze

the diligence of those responsible and in charge and the security measures applied.

The security of personal data is regulated in articles 32, 33 and 34 of the

RGPD, which regulate both the security of the treatment, the 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) processed in such a way as to guarantee adequate security of the personal data.

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

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

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

In this case, according to the reports provided, it is clear that the (...)

It is noteworthy, (...)

In accordance with the evidence available in this initiation agreement,

sanctioning procedure, and without prejudice to what results from the investigation,

it is considered that the known facts could constitute an infraction, im-

attributable to EVERIS, 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 entail the co-
mission of the infractions typified in article 83.5 of the RGPD that under the rubric
"General conditions for the imposition of administrative fines" provides:

“The infractions of the following dispositions will be sanctioned, in accordance with the
section 2, with administrative fines of a maximum of EUR 20,000,000 or, treating-
of a company, of an amount equivalent to a maximum of 4% of the volume of
Total annual global business of the previous financial year, opting for the one with the highest
amount:

a) the basic principles for the treatment, including the conditions for the consent
lien pursuant to 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 are contrary to
ries to this organic law”.

For the purposes of the limitation period, article 72 “Infringements considered very serious”
you see” 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
two 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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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:

-

d) the degree of responsibility of the person in charge or of the person in charge of the

treatment, taking into account the technical or organizational measures that have

applied under articles 25 and 32.

(…)

This shows that EVERIS has not carried out the technical measures

minimum cas when the (...) is found.

-

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

(…)

As a mitigating factor:

-

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

□

(…)

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 personal data processing.

EVERYS is a provider of technological infrastructure management services cas for REIAL AUTOMÒBIL CLUB DE CATALUNYA (hereinafter, RACC), company providing assistance services on behalf of GACM SEGU-ROS GENERALES, COMPAÑÍA DE SEGUROS Y REASEGUROS S.A.U. (GACM) as an assistance reinsurance entity.

Insurance companies or insurance entities manage in the performance of your activity personal data of your clients or insured; already from the same moment of the subscription and selection of risks for life insurance, claims, health, automobile, disability, etc., a large

amount of personal information to be able to process the policies (data medical benefits, bills, death certificates, etc.).

For these reasons, insurers must comply with the protection regulations

data tion. But not only them, the LOPDGDD and the RGPD also apply

insurance brokers, as well as companies involved in the

management of the same, who handle and treat the same types of data

personal.

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 €50,000 (fifty 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

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

variable and seriousness for the rights and freedoms of natural persons, the responsible

The controller and the data processor will apply appropriate technical and organizational measures.

to guarantee a level of security appropriate to the risk, which, where appropriate, includes

yeah, among others:

a) pseudonymization and encryption of personal data;

b) the ability to guarantee the confidentiality, integrity, availability and re-

permanent silence of treatment systems and services;

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

promptly 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

I lie.

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

ta the risks that the treatment of data presents, in particular as a consequence

of the accidental or unlawful destruction, loss or alteration of personal data transmitted

stored, stored or otherwise processed, or unauthorized communication or access

two to said data.

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

certification body approved under article 42 may serve as an element for

demonstrate compliance with the requirements established in section 1 of this

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 having

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 Union Law or

the Member States".

In the present case, at the time of the security breach, there is no evidence

that EVERIS had reasonable security measures based on the possible

ble estimated risks.

(…)

It is clear that EVERIS as a provider of infrastructure management services

technology for RACC did not have the appropriate organizational and technical measures

das to prevent the exposure of personal data of the insured.

Finally,(…).

In accordance with the evidence available in this initiation agreement,

sanctioning procedure, and without prejudice to what results from the investigation,

it is considered that the known facts could constitute an infraction, im-

attributable to EVERIS, 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

sion of the infractions typified in article 83.4 of the RGPD that under the rubric

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

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

section 2, with administrative fines of a maximum of EUR 10,000,000 or, treating-

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

Total annual global business of the previous financial year, opting for the one with the highest

amount:

5)

the obligations of the person in charge and the person in charge in accordance with articles 8,

11, 25 to 39, 42 and 43; (…)”

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

The acts and behaviors referred to in sections 4, 5 and 6 are infractions

of article 83 of Regulation (EU) 2016/679, as well as those that are 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, it is con-

they are considered serious and the infractions that suppose a vulnerability will prescribe after two years.

substantial portion of the items mentioned therein and, in particular, the following:

…

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

be appropriate to ensure a level of security appropriate to the risk of the

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 according to

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

construction, the infringement in question is considered serious for the purposes of the RGPD and

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

establishes article 83.2 of the RGPD:

As aggravating factors:

-

-

d) the degree of responsibility of the person in charge or of the person in charge of the treatment,

taking into account the technical or organizational measures that they have applied in

under articles 25 and 32.

(…)

This shows that EVERIS has not carried out the technical measures

minimum cas when the (...) is found.

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

(...).

As a mitigating factor:

-

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

(…)

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.

EVERYS is a provider of technological infrastructure management services

cas for REIAL AUTOMÒBIL CLUB DE CATALUNYA (hereinafter, RACC),

company providing assistance services on behalf of GACM SEGU-

ROS GENERALES, COMPAÑÍA DE SEGUROS Y REASEGUROS S.A.U.

(GACM) as an assistance reinsurance entity.

Insurance companies or insurance entities manage in the performance

of your activity personal data of your clients or insured; already from the

same moment of the subscription and selection of risks for life insurance,

claims, health, automobile, disability, etc., a large

amount of personal information to be able to process the policies (data

medical benefits, bills, death certificates, etc.).

For these reasons, insurers must comply with the protection regulations

data tion. But not only them, the LOPDGDD and the RGPD also apply

insurance brokers, as well as companies involved in the

management of the same, who handle and treat the same types of data

personal.

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

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

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

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

IX

If the infraction is confirmed, it could be agreed to impose on the person responsible the adoption of

appropriate measures to adjust their actions to the regulations mentioned in this

act, in accordance with the provisions of the aforementioned article 58.2 d) of the RGPD, according to the

which each control authority may “order the person in charge or in charge of the

treatment that the treatment operations comply with the provisions of the

this Regulation, where appropriate, in a certain way and within a

specified period…”. The imposition of this measure is compatible with the sanction

consisting of an administrative fine, as provided in art. 83.2 of the GDPR.

It is warned that not meeting the requirements of this organization may be

considered as an administrative offense in accordance with the provisions of the RGPD,

typified as an infraction in its article 83.5 and 83.6, being able to motivate such conduct the

opening of a subsequent sanctioning administrative proceeding.

Therefore, in accordance with the foregoing, by the Director of the Agency

Spanish Data Protection,

HE REMEMBERS:

FIRST: START A SANCTION PROCEDURE against EVERIS SPAIN S.L., with

NIF B82387770, for the alleged infringement of article 5.1.f) of the RGPD, typified in the

article 83.5 of the RGPD.

START SANCTION PROCEDURE against EVERIS SPAIN S.L. with NIF

B82387770, for the alleged infringement of article 32 of the RGPD, typified in the

article 83.4 of the RGPD.

SECOND: APPOINT R.R.R. as instructor. and, as secretary, to S.S.S.,

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).

THIRD: 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 (€50,000), for the alleged infringement of article 5.1.f) of the

RGPD, typified in article 83.5 of the RGPD.

TWENTY THOUSAND EUROS (€30,000), for the alleged infringement of article 32 of the RGPD, typified in article 83.4 of the RGPD.

FOURTH: NOTIFY this agreement to EVERIS SPAIN S.L., with NIF B82387770, 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).

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 64,000.00 euros, 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 64,000.00 euros and its payment will 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 of the responsibility is revealed within the period granted to formulate

arguments at the opening of the procedure. The voluntary payment of the referred amount

in the previous paragraph may be done at any time prior to the resolution. In

In this case, if it were appropriate to apply both reductions, the amount of the penalty would be

set at 48,000.00 euros.

In any case, the effectiveness of any of the two reductions mentioned will be

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

administrative against the sanction.

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

indicated above (64,000.00 euros or 48,000.00 euros), you must make it effective

by depositing it in account number ES00 0000 0000 0000 0000 0000 open to

name of the Spanish Agency for Data Protection in the bank

CAIXABANK, S.A., indicating in the concept the reference number of the

procedure that appears in the heading of this document and the cause of

reduction of the amount to which it is accepted.

Likewise, you must send proof of payment to the General Subdirectorate of

Inspection to proceed with the procedure in accordance with the quantity

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

performances; in accordance with the provisions of article 64 of the LOPDGDD.

In compliance with articles 14, 41 and 43 of the LPACAP, it is noted that, in what

successively, the notifications sent to you will be made exclusively in a

electronically by appearance at the electronic headquarters of the General Access Point of

the Administration or through the unique Authorized Electronic Address and that, if not

access them, their rejection will be recorded in the file, considering the

processing and following the procedure. You are informed that you can identify before this

Agency an email address to receive the notice of commissioning

disposition of the notifications and that the lack of practice of this notice will not prevent

that the notification be considered fully valid.

Finally, it is pointed out that in accordance with the provisions of article 112.1 of the

LPACAP, there is no administrative appeal against this act.

Sea Spain Marti

Director of the Spanish Data Protection Agency

935-110422

>>

SECOND: On August 24, 2022, the claimed party has proceeded to pay

of the sanction in the amount of 64,000 euros using one of the two

reductions provided for in the Start Agreement transcribed above. Therefore, it has not

acknowledgment of responsibility has been confirmed.

THIRD: The payment made entails the waiver of any action or resource in via

against the sanction, in relation to the facts referred to in the

Home 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 and 48.1 of the Law
Organic 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 Data Protection Agency.
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 EXP202102640, of

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

SECOND: NOTIFY this resolution to NTT DATA SPAIN, S.L.U.

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

937-240122

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es