 File No.: PS/00080/2022

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 May 3, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate sanction proceedings against DKV SEGUROS Y

REINSURANCE, S.A.E. (hereinafter, the claimed party), through the Agreement that is

transcribe:

<<

File No.: PS/00080/2022

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: Ms. A.A.A. (hereinafter, the complaining party), on February 4,

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

claim is directed against DKV SEGUROS Y REASEGUROS, SOCIEDAD

ANONIMA ESPAÑOLA with NIF A50004209 (hereinafter, the claimed party). The

The grounds on which the claim is based are as follows:

The claim is received through the Catalan Data Protection Authority

indicating that the facts are not included within the assumptions on which

who has competition. The claimant states that she has received at her email address

e-mail, on numerous occasions, authorizations for medical tests of

unknown third parties. In some cases, the type of diagnostic test is included.

Every time he has received an authorization, he has communicated it, forwarding the mail to the entity (authorizations and customer service). It has not been resolved and continues to receive authorizations that do not correspond to you.

Along with the claim, provide a copy of the emails received corresponding to other people and mail exchanges with the claimed revealing the situation.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5 December, Protection of Personal Data and Guarantee of Digital Rights (hereinafter LOPDGDD), said claim was transferred to the claimed party, to proceed with its analysis and inform this Agency within a month, of the actions carried out to adapt to the requirements set forth in the data protection regulations.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of October 1, of the Common Administrative Procedure of the Administrations (hereinafter, LPACAP), by electronic notification, was received in dated March 12, 2021, as stated in the certificate in the file.

On April 11, 2021, this Agency received a written response indicating (...).

THIRD: On June 14, 2021, 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

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:

First of all, it is verified that there are no breach notifications sent

by the claimed to this Agency.

It is verified that the claimant provides conversations held by email

with the claimed, of different dates. The first conversation provided contains the

following documents:

- Email received on 10/08/2020 corresponding to a third person. In

the mail appears the name and surname of the third person and an indication of the

authorization sent: “This document is password protected for security,

being the NIF of the client for which the authorization is requested.” It also says "Yes.

If you need any clarification or information in this regard, we will assist you through the

email ***EMAIL.1.”

- Reply to it, to the indicated address ***EMAIL.1 indicating that you do not

corresponds.

- Respondent's reply to this reply from the claimant with the text "In

We are currently working on your request…”.

- Second response from the respondent indicating "we inform you that you must contact

contact your branch … ***EMAIL.2…”

- Reply email from the claimant to the claimant, forwarding all the

mail history to the indicated address “***EMAIL.2”

- Response from the respondent to the claimant indicating that "We regret not being able to assist you at this time since we do not have the documentation to be able to correctly manage your request."

Provide a sample of other documents related to third-party authorizations people received in your email, emails received on dates 07/10/2020, 10/30/2020 (2:33 p.m.), 10/30/2020 (12:37 p.m.), 12/03/2020 and 01/26/2021.

In the one dated 10/30/2020 (2:33 p.m.), addressed to a "collaborator", the authorization attached without indication that it is password protected, providing the claimant copy of said authorization in which the following information appears, among others:

- Authorization number.
- Data of the insured: name and surnames and policy number.
- Authorization/test data:

"(…)"

"(…)"

On the one dated 10/30/2020 (12:37 p.m.) the attached authorization appears without indication of which is password protected, but the claimant does not provide a copy of the authorization.

Provide a copy of another authorization dated 11/25/2020 in which the following data, among others:

- Authorization number.

- Data of the insured: name and surnames and policy number.

- Authorization/test data:

“(…)”

"(...)".

Provides a copy of an email dated 12/15/2020, sent by the claimant

to four email addresses (***EMAIL.3, ***EMAIL.4, ***EMAIL.5,

***EMAIL.1). In the mail he lists the names of seven people from whom he has received

authorizations, stating that on numerous occasions he receives authorizations

addressed to different people that he does not know or have a relationship with them and that each time

that has received an authorization of this type has notified it, without correcting the

issue.

On the chronology of events.

(...).

Affected data.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

(...).

Communication of the incident to those affected.

(...).

Actions taken to resolve the incident and minimize the impact.

(...).

Regarding the qualification of the incident as a security breach of personal data.

(...).

On the security measures of personal data processing adopted

prior to the incident in the data processing involved.

(...).

Measures taken so that a similar incident does not occur again in the future.

(...).

Contract with managers.

(...).

Contract with VIVAZ.

(...).

Origin of the incident.

(...).

FIFTH: In view of the reported facts and in accordance with the evidence

available at this time, the Data Inspection of this Spanish Agency

of Data Protection considers that the processing of personal data carried out by

claimed party would not meet the conditions imposed by current regulations in

matter of data protection, so it is appropriate to open this procedure

sanctioning lie.

FOUNDATIONS OF LAW

FIRST: In accordance with the powers that article 58.2 of the 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 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.”

SECOND: Article 5.1.f) of the RGPD establishes the following:

“Article 5 Principles relating to processing:

1. The personal data will be:

(…)

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

including protection against unauthorized or unlawful processing and against

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

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

In relation to this principle, Recital 39 of the aforementioned GDPR states that:

“[…]Personal data must be processed in a way that guarantees security and

appropriate confidentiality of personal data, including to prevent access

or unauthorized use of said data and of the equipment used in the treatment”.

The documentation in the file offers clear indications that the

claimed violated article 5.1 f) of the RGPD, principles related to treatment.

In the specific case under examination, it is clear that the respondent party sent, from the

April 16, 2020 to March 9, 2021, to third person, 51 emails

They weren't addressed to her.

Indeed, as evidenced in the file, it is clear that the claimant received (...).

On the other hand, the respondent party acknowledged the facts, stating to this Agency

than the incident (...), also concluding (...).

THIRD: Article 4.12 of the RGPD establishes that it is considered "violation of the

security of personal data: any breach of security that causes the

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

stored or otherwise processed, or unauthorized communication or access to

said data."

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

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

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

variable probability and severity for the rights and freedoms of individuals

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

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

which in your case includes, among others:

a) pseudonymization and encryption of personal data;

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

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

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

of the technical and organizational measures to guarantee the security of the treatment.

2. When evaluating the adequacy of the security level, particular consideration shall be given to taking 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 (The underlining is from the AEPD).

Recital 75 of the RGPD lists a series of factors or assumptions associated with risks for the guarantees of the rights and freedoms of the interested parties:

"The risks to the rights and freedoms of natural persons, serious and variable probability, may be due to the processing of data that could cause physical, material or non-material damages, particularly in cases where that the treatment may give rise to problems of discrimination, usurpation of identity or fraud, financial loss, reputational damage, loss of confidentiality of data subject to professional secrecy, unauthorized reversal of the pseudonymization or any other significant economic or social damage; in the cases in which the interested parties are deprived of their rights and freedoms or are prevent exercising control over your personal data; In cases where the data treated personalities reveal ethnic or racial origin, political opinions, religion or philosophical beliefs, militancy in trade unions and the processing of genetic data, data relating to health or data on sex life, or convictions and offenses criminal or related security measures; In cases where they are evaluated personal aspects, in particular the analysis or prediction of aspects related to the performance at work, economic situation, health, preferences or interests personal, reliability or behavior, situation or movements, in order to create or use personal profiles; in the cases in which personal data of vulnerable people, in particular children; or in cases where the treatment

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

interested."

From the actions carried out, there is evidence of the existence of reasonable indications and

enough that the security measures, both of a technical nature and

organizations, with which the claimed party had in relation to the data of

health subject to treatment, were not adequate at the time of occurrence

improper access.

The consequence of this implementation of deficient security measures was the

Exposure to a third party of personal data relating to the health of

other customers, that is, those affected have been deprived of control over their

personal information.

It should be added that, in relation to the category of data to which the third person

outside has had access, they are in the category of special according to what

provided in art. 9 of the RGPD, a circumstance that supposes an added risk that

must assess in the risk management study and that increases the degree requirement

of protection in relation to the security and safeguarding of the integrity and

confidentiality of these data.

This risk must be taken into account by the data controller, who must

establish the necessary technical and organizational measures to prevent the loss of

control of the data by the data controller and, therefore, by the data controllers.

holders of the data that provided them.

The fact that workers of two different managers have committed the same

error shows that it is not a specific human error, but a faulty

CRM configuration, which shows that these errors are just the

sample of the lack of security measures adopted by the person in charge.

FOURTH: Article 33 of the RGPD, Notification of a violation of the security of

personal data to the control authority, establishes that: “1. In case of violation

of the security of the personal data, the person in charge of the treatment will notify it to

the competent supervisory authority in accordance with article 55 without delay

wrongful and, if possible, no later than 72 hours after you had

record of it, unless it is unlikely that the security breach

constitutes a risk to the rights and freedoms of natural persons. If the

notification to the control authority does not take place within 72 hours, it must go

accompanied by an indication of the reasons for the delay.

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

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

be aware.

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 approximate number of

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

affected personnel;

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

treatment to remedy the violation of the security of personal data,

including, if applicable, the measures adopted to mitigate the possible effects

negatives.

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

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

5. The data controller will document any violation of the

security of personal data, including the facts related to it, its

effects and corrective measures taken. Such documentation will allow the

control authority verify compliance with the provisions of this article.

Although it is true that the entity claimed was aware of the incident, it adopted measures

tending to remedy the same, article 33 of the RGPD establishes

explicit that security breaches, provided that in a breach they are affected

personal data and implies a risk for the rights and freedoms of the

natural persons, must be notified by the data controller within the period of

72 hours after you have received proof of it to the Control Authority

(AEPD), a circumstance that would be fulfilled in the present case, since, in addition, the

Affected data belongs to the category of data regulated in article 9.1 of the

cited RGPD (Treatment of special categories of personal data).

In the present case, it is known that the respondent has suffered a security breach of

personal data having proof of it since July 13, 2020 and not

has notified this Agency. A rape can have a number of adverse effects

considerable in people, likely to cause damage and physical harm,

material or immaterial. The GDPR explains that these effects may include the

loss of control over your personal data, the restriction of your rights, the

discrimination, identity theft or fraud, financial loss,

unauthorized reversal of pseudonymization, reputational damage and loss

confidentiality of personal data subject to professional secrecy. also can

include any other significant economic or social harm to those persons.

Lastly, the controller himself states that (...) has caused

that the facts claimed to this Agency occurred, but the truth is that the

complainant brought the incident to the attention of the entity complained against, and the latter did

ignore the notice.

In accordance with the foregoing, it is estimated that the entity's actions could

suppose the violation of article 33 of the RGPD, an infraction typified in its article

83.4.a) of the same legal text.

FIFTH: In accordance with the evidence available in this

moment of agreement to initiate the sanctioning procedure, and without prejudice to what

result of the instruction, it is considered that the claimed party would fail to comply with the provisions

in article 5.1.f) of the RGPD, which could lead to the commission of an infringement

typified in article 83.5 of the RGPD.

The lack of implementation of technical and organizational measures necessary to

guarantee an adequate level of security in the processing of personal data

could constitute, on the part of the claimed entity, an infringement of the provisions of the article 32 of the RGPD, typified in article 83.4.a) of the RGPD.

Likewise, failure to comply with the duty to notify the data protection authority data a violation of personal data security, could constitute an infringement of the provisions of article 33 of the Regulation, typified in article 83.4.a) of the same legal text.

SIXTH: Article 83.5 of the RGPD provides the following:

"5. Violations of the following provisions will be sanctioned, in accordance with the paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a company, an amount equivalent to a maximum of 4% of the global total annual turnover of the previous financial year, opting for the largest amount:

a)

the basic principles for the treatment, including the conditions for the consent under articles 5, 6, 7 and 9;”

For its part, article 71 of the LOPDGDD, under the heading "Infringements" determines what following: "The acts and behaviors referred to in the sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to this organic law.”

For the purposes of the limitation period for infractions, article 72 of the LOPDGDD, under the rubric of infractions considered very serious, it establishes the following: “1. In 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.”

The violation of articles 32 and 33 RGPD is typified in the article

83.4.a) of the aforementioned RGPD in the following terms:

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

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

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

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

the largest amount:

a)

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

11, 25 to 39, 42 and 43.”

(…)

For the purposes of the limitation period for infractions, article 73 of the LOPDGDD,

under the heading "Infringements considered serious", it establishes the following:

“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 result

appropriate to guarantee a level of security appropriate to the risk of the treatment,

in the terms required by article 32.1 of Regulation (EU) 2016/679.

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

a breach of security of personal data in accordance with the provisions of

Article 33 of Regulation (EU) 2016/679.

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

83.5 and 83.4 of the GDPR, transcribed above.

SEVENTH: In order to determine the administrative fine to be imposed, the

the provisions of articles 83.1 and 83.2 of the RGPD, precepts that indicate:

"1. Each control authority will guarantee that the imposition of fines

administrative actions under this article for violations of this

Regulation indicated in sections 4, 5 and 6 are in each individual case

effective, proportionate and dissuasive.

2. Administrative fines will be imposed, depending on the circumstances of each

individual case, in addition to or as a substitute for the measures contemplated in the

Article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine

administration and its amount in each individual case will be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the nature

nature, scope or purpose of the processing operation in question, as well as the number

number of interested parties affected and the level of damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor to pa-

allocate the damages suffered by the interested parties;

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

gives an account of the technical or organizational measures that have been applied by virtue of the

articles 25 and 32;

e) any previous infringement committed by the person in charge or the person in charge of the treatment;

f) the degree of cooperation with the supervisory authority in order to remedy the

infringement and mitigate the possible adverse effects of the infringement;

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

h) the way in which the supervisory authority became aware of the infringement, in particular

whether the person in charge or the person in charge notified the infringement and, if so, to what extent.

gives; i) when the measures indicated in article 58, section 2, have been ordered

given previously against the person in charge or the person in charge in question in relation to

the same matter, compliance with said measures;

j) adherence to codes of conduct under Article 40 or to certification mechanisms

approvals approved in accordance with article 42,

k) any other aggravating or mitigating factor applicable to the circumstances of the case,

such as financial benefits obtained or losses avoided, directly or indirectly.

mind, through infraction."

For its part, article 76 "Sanctions and corrective measures" of the LOPDGDD

has:

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

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

established in section 2 of the aforementioned article.

2. In accordance with the provisions of article 83.2.k) of Regulation (EU) 2016/679

may also be taken into account:

a) The continuing nature of the offence.

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

of personal data.

c) The profits obtained as a result of committing the offence.

d) The possibility that the conduct of the affected party could have induced the

commission of the offence.

e) The existence of a merger by absorption process after the commission

of the infringement, which cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

g) Have, when it is not mandatory, a delegate for the protection of

h) The submission by the person in charge or person in charge, with

voluntary, to alternative conflict resolution mechanisms, in those

assumptions in which there are controversies between those and any

interested."

data.

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

In accordance with the transcribed precepts, and without prejudice to what results from the

instruction of the procedure, in order to set the amount of the penalty for infringement

of article 5.1 f), it is appropriate to graduate the fine taking into account:

As an aggravating circumstance:

Article 83.2.a) RGPD: the nature, seriousness and duration of the infringement, taking

taking into account the nature, scope or purpose of the processing operation to be carried out.

concerned, as well as the number of interested parties affected and the level of damages

who have suffered:

The error is maintained from 04/16/2020 to 03/09/2021.

Likewise, the claimant repeatedly informed the respondent

the situation, without it acting in any way until receiving the transfer of the

claim-"(…)"

Regarding the volume of treatments carried out, the claimant receives 51 emails

emails of 32 different affected.

Article 83.2 g) RGPD: the categories of personal data affected by

the infringement; whenever special categories of personal data have been affected.

sound. In this sense, the RGPD always grants the treatment of these data, a

special protection and consideration. Thus, Recital 75 of the RGPD considers the

treatment of data related to health, such as risk treatment.

Sanction for the infringement of article 32 of the RGPD.

In accordance with the transcribed precepts, and without prejudice to what results from the

instruction of the procedure, in order to set the amount of the penalty for infringement

of article 32 of the RGPD, it is appropriate to graduate the fine taking into account:

As aggravating factors:

Article 83.2 g) RGPD: the categories of personal data affected by

the infringement; whenever special categories of personal data have been affected.

sound. In this sense, the RGPD always grants the treatment of these data, a

special protection and consideration. Thus, Recital 75 of the RGPD considers the

treatment of data related to health, such as risk treatment.

Article 76.2 a) LOPDGDD: “The continuing nature of the infraction.” It is noteworthy the

continuing nature of the offence. The error is maintained from 04/16/2020 to

03/09/2021.

Article 76.2 b) LOPDGDD: "The link between the activity of the offender and the

tion of personal data processing". The activity of the claimed entity requires

continuous processing of personal data. Likewise, the entity claims

da carries out for the development of its activity, a high volume of damage treatment

personal cough.

Sanction for the infringement of article 33 of the RGPD.

Article 83.2 g) RGPD: the categories of personal data affected by

the infringement; whenever special categories of personal data have been affected.

sound. In this sense, the RGPD always grants the treatment of these data, a

special protection and consideration. Thus, Recital 75 of the RGPD considers the

treatment of data related to health, such as risk treatment.

Article 76.2 b) LOPDGDD: "The link between the activity of the offender and the

tion of personal data processing". The activity of the claimed entity requires

continuous processing of personal data. Likewise, the entity claims

da carries out for the development of its activity, a high volume of damage treatment

personal cough

It is known that the claimed person suffered a personal data security breach

having proof of it since July 13, 2020 and did not notify this

Agency.

Considering the exposed factors, the initial valuation that reaches the amount of the

fine is €100,000 for infringement of article 5.1 f) of the RGPD, regarding the

violation of the principle of confidentiality and €60,000 for each of the

violations of articles 32 and 33 of the aforementioned RGPD, regarding the security of the

treatment of personal data.

EIGHTH: Establishes Law 40/2015, of October 1, on the Legal Regime of the Sector

Public, in Chapter III on the "Principles of the power to sanction", in the

Article 28 under the heading "Responsibility", 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 their capacity to

to act, the affected groups, the unions and entities without legal personality and the

independent or autonomous estates, which are responsible for them

title of fraud or guilt."

Lack of diligence in implementing appropriate security measures

with the consequence of breaching the principle of confidentiality constitutes the

element of guilt.

NINTH: If the infraction is confirmed, it could be agreed to impose the

adoption of appropriate measures to adjust its actions to the aforementioned regulations

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

according to 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:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

FIRST: START A SANCTION PROCEDURE against DKV SEGUROS AND

REASEGUROS, SOCIEDAD ANONIMA ESPAÑOLA, with NIF A50004209, by the

alleged infringement of article 5.1. f) of the RGPD, typified in accordance with the provisions of

Article 83.5 of the RGPD, qualified as very serious for the purposes of prescription in the

Article 72.1 a) of the LOPDGDD.

SECOND: START A SANCTION PROCEDURE against DKV SEGUROS AND

REASEGUROS, SOCIEDAD ANONIMA ESPAÑOLA, with NIF A50004209, by the

alleged infringement of article 32 of the RGPD, typified in accordance with the provisions of the

article 83.4 of the aforementioned RGPD, qualified as serious for the purposes of prescription in the

Article 73 section f) of the LOPDGDD.

THIRD: START A SANCTION PROCEDURE against DKV SEGUROS AND

REASEGUROS, SOCIEDAD ANONIMA ESPAÑOLA, with NIF A50004209, by the

alleged infringement of article 33 of the RGPD, typified in accordance with the provisions of the

article 83.4 of the aforementioned RGPD, qualified as serious for the purposes of prescription in the

Article 73 r) of the LOPDGDD.

FOURTH: APPOINT instructor to B.B.B. and, as secretary, to C.C.C., indicating that

any of them may be challenged, where appropriate, in accordance with the provisions of the

Articles 23 and 24 of Law 40/2015, of October 1, on the Legal Regime of the Sector

Public (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: THAT for the purposes provided in art. 64.2 b) of Law 39/2015, of 1 October, of the Common Administrative Procedure of the Public Administrations, the The corresponding sanction would be €100,000 for infraction of article 5.1 f) of the RGPD, regarding the violation of the principle of confidentiality and €60,000 for each of the infractions of articles 32 and 33 of the aforementioned RGPD, with respect to the security of the processing of personal data, without prejudice to what results from The instruction.

SEVENTH: NOTIFY this agreement to DKV SEGUROS Y REASEGUROS, SPANISH LIMITED COMPANY, with NIF A50004209, granting it a term of hearing of ten business days to formulate the allegations and present the tests you deem appropriate. In your statement of arguments, you must provide your NIF and the procedure number that appears in the heading 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 penalty would be established at ONE HUNDRED AND SEVENTY-SIX THOUSAND EUROS
(€176,000) 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 penalty would be established at ONE HUNDRED AND SEVENTY-SIX THOUSAND EUROS
(€176,000) 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 ONE HUNDRED AND THIRTY-TWO THOUSAND EUROS (€132,000.)
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 (80,000 euros or 36,000 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.

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

935-150322

>>

SECOND: On May 28, 2022, the claimed party has proceeded to pay

of the sanction in the amount of 132,000 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 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 PS/00080/2022, of

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

SECOND: NOTIFY this resolution to DKV SEGUROS Y REASEGUROS,

S.A.E.

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

936-240122

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es