 File No.: EXP202201254

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 February 28, 2023, the Director of the Spanish Agency for

Data Protection agreed to initiate sanction proceedings against PELAYO MUTUA DE

FIXED PREMIUM INSURANCE AND REINSURANCE (hereinafter, the claimed party),

through the Agreement that is transcribed:

<<

File No.: EXP202201254

AGREEMENT TO START THE SANCTION PROCEDURE

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

based on the following

FACTS

FIRST: A.A.A. (hereinafter, the claimant) on 12/1/2021 files

claim before the Spanish Data Protection Agency (AEDP). The

The claim is directed against PELAYO, MUTUA DE SEGUROS Y REASEGUROS A

FIXED PREMIUM, with NIF G28031466 (hereinafter, the claimed party or the

INSURANCE CARRIER).

The reason on which the claim is based is that on 09/22/2021, without your

consent, the INSURER provided a third party with their identity data

(name, surname, NIF, address and telephone number); information regarding the

insurance policy of which she was the policyholder and insured; information of the

declared claims and information on the insurance premium (amount, date of

maturity and payment date). The third party to whom the data was communicated was the

person with whom the claimant had signed a deposit contract for the sale of the

insured vehicle and which is identified in some documents as “B.B.B.

buyer" (hereinafter, the third party). The claimant states that the facts

they took place in an office of the INSURER "located at ***ADDRESS.1".

Thus, the claimant states that on 11/27/2020 it contracted with the INSURER

all-risk insurance for your vehicle; which in September 2021 began

negotiations for the sale of the vehicle and that on 09/22/2021 received from the third party

through WhatsApp a copy of a document with the name of the INSURER that

contained personal data and data from the insurance policy. After what happened, he presented

claim on 09/23/2021 before the INSURER.

Provide with your claim, in addition to the copy of the DNI, these documents:

-Several screenshots of a mobile terminal with WhatsApp messages that

sends the third. The date 09/22/2021 appears on all captures:

 Some text messages sent between 1:50 p.m. and 1:54 p.m.

the following content: "I have not uploaded the paper that they gave me in

Pelayo, I'll send it to you later”; “They have also given me a free phone number

Pelayo for you to call and try to solve them for you”; "They told me no.

You can assign me the remaining insurance until the end of the insurance”; "What do you have?

to unsubscribe so that I leave mine done, that I wanted to leave it done in

these days"

Image of the document that the worker of the agent of the INSURANCE COMPANY

handed over to the third. The policy number is stated in that document

"***POLICY.1" "Pelayo Mutua de Seguros" and the following information distributed

in these headings:

"Customer data": which includes the name and two surnames of the claimant, his

NIF, mobile phone number, address and nationality.

"Policy data": which contains the date of the policy, registration, make and model

vehicle.

"Claims": Four claims appear reflected on which their information is facilitated.

respective identification number, the date on which it occurred and the date on which it was

stated. The last two registered are:

Yo. Number XXXXXXXX, occurred on 08/29/2021 and declared on 09/06/2021.

ii. Number XXXXXXXXX, occurred on 08/26/2021 and declared on 08/26/2021.

-Conditions of the insurance contract: The clauses of the conditions that detail the

risks excluded from coverage in the policy *** POLICY.1 and a document related to the

"Modification of automobile insurance *** POLICY.1", which entered into force on 11/17/2020

and that it refers to the vehicle on which the facts relate.

- Letter that the claimant's lawyer addressed to the INSURER on 09/23/2021.

- Written response from the INSURER, dated 10/11/2021. In essence, it claims that

the office where the events occurred belonged to an agent and not to the company itself.

That the agent's employee provided the third party with the data on the basis of interest

of the third party, since the latter provided a deposit contract signed with the

claimant, for which reason it was in their interest to declare this incident. alleges,

likewise, that the third party was already aware of the claimant's data through the

earnest money contract signed with her and that, since she had the vehicle in her possession, it was logical to think that he had accessed the vehicle's documentation.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5 December, Protection of Personal Data and guarantee of digital rights (in hereafter LOPDGDD), said claim was forwarded to the INSURER for to proceed with its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements established in the regulations of Data Protection.

The notification was made electronically, in accordance with Law 39/2015, of 1 October, of the Common Administrative Procedure of Public Administrations (in hereinafter, LPACAP) being the date of availability and acceptance, respectively, on February 2 and 3, 2022. This is stated in the certificate issued by the Support service for the Electronic Notification Service and Electronic Address Authorized by the FNMT that is in the file (hereinafter, FNMT certificate)

The INSURER responds to the information request on 03/01/2022. request proceed to file the procedure as it has been accredited that it has not there has been no violation of the right of the claimant in terms of protection of data.

In defense of his claim, he argues that the agent's employee provided the third party with the data on the basis of the legitimate interest that it held, since it provided a earnest money contract signed with the claimant, for which reason the declaration was of interest

of that accident. That the third party was already aware of the claimant's data through

through the deposit contract entered into with her and that, since she had the vehicle in

his power it was logical to think that he had accessed the documentation of the vehicle.

He also makes these statements:

-Reiterates that it is false that the information was provided by an employee of the

INSURANCE CARRIER. The information was provided by an employee of the CUSEGUR agent

2015, AGENCIA DE SEGUROS, S.L., mediator with which the insurance company

had signed the corresponding Agency contract and that it carried out its activity

in the office located in the city of XXXXXX.

-That it is false that the claimant began negotiations for the sale of the vehicle

in September 2021, since he has stated on various occasions that as of

08/27/2021 I had already signed the deposit contract. It alludes to the recording of a

conversation held by the claimant with a teleoperator from the

INSURANCE CARRIER.

-That, once the claim was received, he contacted the agent and his employee/commercial, who

had provided the data to the third party, who informed him that a

sir to request a price for a car insurance for which he already had subscribed

a deposit contract for the sale of the vehicle dated 08/27/2021 and informed the

commercial that the car was already in his possession. That when he gave the vehicle data

to calculate the insurance estimate, you were informed that this vehicle had a

policy in force at the INSURANCE COMPANY and that, until the cancellation is given due to the

The policyholder (the claimant) could not insure the vehicle in her name.

That days later the third party returned to the office to take out the insurance and

He commented again that "the policy was still in force, that the

It is still low and they were also claiming a claim from us. It is before this information

when the [third party] requests that they be provided with a printout of the screen, since as

previously exposed had stated that the car was in his possession with

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

4/22

date prior to the one that was recorded as the date of occurrence of the accident (8/29/2021).”

That the third party told the agent's business that he needed a copy of the

document to speak with the workshop and the insured (the claiming party) to

teach them that on August 29 there was a claim in case they were defrauding him.

-It mentions other issues, such as the DNI of the lawyer of the claimant who

sent by letter to the INSURER coincides with that of the person listed as

contrary in the friendly claim report declared by the claimant and which gave rise to

to provide the third party with information regarding the insurance of the vehicle. that does not have

sense that the third party provided the claimant via WhatsApp with a screenshot with the

informative document obtained from the agent's commercial if it was not to ask

explanations of the facts, for which reason it proposes that the claimant be required to

that provides the entire conversation maintained through WhatsApp with the third party and

not the selection you provided.

Provide a copy of the email exchanged between the Commercial Manager of the

Insurer and the exclusive agent on 09/29/2021 in order to clarify the

facts that are the subject of the claim.

THIRD: On 03/1/2022, in accordance with article 65 of the LOPDGDD,

The claim presented by the complaining party was admitted for processing.

The claimant was notified of the admission for processing of the claim by mail

postal on 03/1/2022 and received on 03/10/2022. This is confirmed by the certificate that

work on file.

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

preliminary investigation actions to clarify the facts under

of the functions assigned to the control authorities in article 57.1 and of the

powers granted in article 58.1, both of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter GDPR), and in accordance

with the provisions of Title VII, Chapter I, Second Section, of the LOPDGDD. HE

is aware of the following points that appear in the Report of

Inspection, from which this fragment is transcribed:

<<RESULT OF INVESTIGATION ACTIONS

In order to investigate the occurrence of the events described, on April 22,

2022 a request for information was made to each of the identified entities

in the previous heading.

The responses to these requirements were entered into the electronic headquarters of the

Spanish Data Protection Agency dated May 5, 2022. And the

The most relevant information provided is the following:

- Agency agreement

The documentation provided by the INSURER certifies that, through the

Agency Contract signed with the AGENT on February 1, 2014, the

AGENT agrees to carry out its mediation activity on an insurance portfolio

property of the INSURER and manage it, in addition to carrying out new production

for the INSURER as Exclusive Insurance Agent. Also attached is the

Annex to the Agency Contract with the new conditions regarding the protection of

data signed on May 9, 2018 and the Agency Contract Resolution

communicated by the AGENT dated January 31, 2022, date from which the

AGENT no longer provides insurance distribution services for the INSURER.

- AGENT response

In relation to the claim filed by the claimant, the AGENT

states:

"That nothing has had to do with the subscription of the aforementioned policy or with the person

indicated (claiming party). That said person (complaining party) was never attended to

in the office in the office that this company has in Cuenca in its capacity as Agency

of the INSURER, nor has he had any relationship with the company. […]".

- Validity of the claimant's car insurance policy

The INSURER informs that the car insurance was in force until the

11/16/2021 in the name of the claimant, that the insurance was canceled at expiration and that the

INSURER does not have a contract signed with the new acquirer.

The telephone recording of the conversation held on 08/27/2021 is provided at

15:11 hours between the INSURER and the claiming party.

-

-

-

The complaining party informs that his vehicle has been sold, that he has

signed the deposit contract and that he is going to sign the purchase contract on

09/30/2021.

The operator of the INSURER informs you that in order to deal with your

request to cancel the insurance from that date, in advance,

due to the transfer of the vehicle, you must send a signed letter to

the company with a copy of your ID, photocopy of the sales contract or

photocopy of the registration certificate already transferred to the person who had

purchased the vehicle (providing the email address corresponding to

these effects).

The claiming party states that the buyer wants to insure the car with

the INSURER to all risks and the operator reiterates that for this it is

It is necessary for the claiming party to first process the withdrawal.

The INSURER indicates that the claimant sent an email to Pelayo on

09/21/2021, to the email address requestbaja@pelayo.com, providing

copy of your ID and a letter signed dated 08/27/2021 "for the purpose of processing the

Non-renewal of the vehicle insurance contracted with you. The letter is sent and

it is found that the claimant also states "That I intend to

to sell the described vehicle. With contract of sale commitment of date

08/27/2021 and subsequent purchase contract dated 09/30/2021". THE INSURER

indicates that it did not provide either of the two contracts.

- Claims occurred on the dates of 08/26/2021 and 08/29/2021

1. Claim 21147277 with date of occurrence: 08/26/2021

Declaration date: 08/26/2021

Form of statement: by phone call, recording is provided.

Accident data:

[…] the interested party states that she has sold the car and needs to repair it

urgent for this reason, because it cannot be delivered like this to the person who has

bought.

Likewise, he refers that he needs a workshop to repair it as soon as possible, so

you are offered the possibility of taking the vehicle to a guaranteed workshop that works with

Pelayo, what he accepts, facilitating himself, therefore, an appointment with the workshop: AUTOMOTIVE

RYCAUTO S.L. located at XXXXXX, for the next day, 8/27/2021.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

6/22

A recording of the telephone conversation held by the party is provided.

claimant with the INSURER dated 08/27/2021 where the party

The claimant states that "...Yesterday I gave reports... and I took it today (to the workshop), I

They have appraised it and they have to fix it for me so that the car is in

conditions. I know that this gentleman is going to take out the insurance with you…".

1. Claim 21152561 with date of occurrence: 08/29/2021

Declaration date: 09/06/2021

Form of declaration: claim received from the opposing company

Accident data: This accident is recorded on 9/6/2021 for the claim of

Allianz, insurance company of the other vehicle involved in the accident, received at

through the computer system, which indicated that the incident had occurred

dated 08/29/2021.

The opponent that appears in the friendly declaration of the accident is the lawyer

that appears on the seal of a letter dated 09/23/2021 directed by the party

claimant to the INSURER.

On June 16 and July 8, 2022, the AUTOMOTIVE workshop is requested

RYCAUTO S.L. located at XXXXXX information related to the management of repairs

of the claiming party's vehicle. On June 22 and July 14, 2022 they have

entry into the electronic office of the AEPD the respective answers. Next,

the transferred information is exposed.

- In relation to the clarification requested as to whether on 08/27/2021 the vehicle

referred to was taken to the workshop and for what reason, for appraisal and/or repair and

In the event that it has been so, accreditation of the person who carried out the

delivery of the vehicle, person who removed it and date of removal. The workshop

conveys that the claiming party is the person who delivers the vehicle for

photoperitary, but the date is not recorded since, in internal protocol, when a

vehicle is taken to photoperitary, no note is taken in the database,

exception of the telephone to notify the client when it has been assessed and can go to

pick it up.

- In relation to the second accident, provide the following information:

o Expert report date: 09/06/2021 at 11:28 p.m.

o Expert photo: C.C.C., DNI ***NIF.1

o Expert Pelayo: D.D.D.

o Person who delivers and picks up the vehicle from the workshop

or there is no date

: B.B.B., E.E.E., DNI

***NIF.2

of delivery or removal of the vehicle, it is presumed that the

vehicle is delivered on 09/06/2021 since it is the date on

that the Reparation Order is opened. There is no collection date.

only date of payment by transfer on 09/15/2021. He

vehicle is picked up by B.B.B., E.E.E., but we do not know the date since the

employee and receptionist C.C.C., that whoever makes said delivery no longer

works at Rycauto Automotive.

C / Jorge Juan, 6

- Provide Vehicle Repair Order dated 09/06/2021 addressed to B.B.B.,

E.E.E. and invoices addressed to the INSURER dated 09/10/2021 and to the

claiming party dated 09/23/2021, where it is indicated paid and reflects the

transfer date, 09/15/2021.

On June 7, 2022, collaboration is requested from the General Directorate of

Traffic, DGT, for the identification of the holders of the vehicle referred to in this

file from November 17, 2020 to the present. Dated 1 of

July 2022, the DGT reports that said vehicle was registered in Spain with

dated October 25, 2017 by the claimant and that on October 29,

2021 it was transferred to its current owner, Mrs. XXX, with NIF ********X.

On June 7, 2022, a request for

information related to the facts denounced, among which is included the contract of

earnest money This information requirement, which has an acknowledgment date of 15

June 2022 has not been attended to within the term or on the date of writing this

report.

- In the email provided, the AGENT states that “B.B.B. buyer" asked the

screen print with the claiming party's car insurance policy

when he verified that he could not take out the insurance for the car with the license plate of the

vehicle of the claiming party that he had purchased, because that license plate

She was still active in the INSURER, and she feared that they were defrauding her.

- A fact was verified that aroused the suspicion of fraud in “B.B.B.

buyer", dated 09/06/2021, the claimant declares to the

INSURER an accident that occurred on 08/29/2021, a date after the

The claiming party states that they have signed the deposit contract for the sale

of your vehicle, 08/27/2021.>>

FUNDAMENTALS OF LAW

Yo

Competence

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

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

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

LOPDGDD, is competent to initiate and resolve this procedure the Director of the

Spanish Data Protection Agency.

Article 63.2 of the LOPDGDD determines that "The procedures processed by the

Spanish Data Protection Agency will be governed by the provisions of the

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

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures."

II

applicable provisions

The GDPR refers to the principles that govern the processing of personal data.

personal nature in article article 5, "Principles relating to treatment", which

has:

"1. Personal data will be:

[…]

f) processed in such a way as to guarantee adequate data security

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

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

or appropriate organizational ("integrity and confidentiality");

[…]

2. The controller will be responsible for compliance with the provisions of

paragraph 1 and able to demonstrate it ("proactive responsibility")."

Article 32 of the GDPR, "Security of treatment", establishes that:

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

nature, scope, context and purposes of processing, 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 and

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

which may include, among others:

a) the pseudonymization and encryption of personal data;

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

permanent treatment systems and services;

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

quickly in the event of a physical or technical incident;

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

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

2. When evaluating the adequacy of the security level, particular consideration will be given to

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

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

personal information transmitted, preserved or processed in another way, or the communication or unauthorized access to such data.

3. Adherence to an approved code of conduct pursuant to 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 controller and the processor shall take measures to ensure that any person acting under the authority of the controller or processor and have access to personal data can only process such data by following instructions of the person in charge, unless it is obliged to do so by virtue of the Law of the Union or of the Member States.

II

Responsible for the treatment

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

The claimed INSURER is responsible for the alleged violations of the GDPR that give rise to the opening of this sanctioning procedure had an account of their status as controller of the treatment carried out.

Article 4 of the GDPR, "Definitions", refers in section 7 to the person responsible for the treatment or responsible as "the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the ends and means of the treatment; if the law of the Union or of the Member States determines the purposes and means of treatment, the person in charge of the treatment or the specific criteria for

their appointment may be established by the Law of the Union or of the States

members".

Likewise, article 4.8 of the GDPR defines the person in charge of the treatment or person in charge

as “the natural or legal person, public authority, service or other body that

process personal data on behalf of the data controller”.

The insurance sector regulations contain specific provisions on the position

who occupy, as data controller or data processor, the

different subjects involved in the insurance distribution activity. Is

Therefore, it is necessary to refer to Royal Decree-Law 3/2020, of February 4, of

“urgent measures for the incorporation into the Spanish legal system of various

directives of the European Union", (hereinafter R.D-law 3/2020) whose Second Book

is dedicated to the "Measures for the adaptation of Spanish law to the regulations

of the European Union in matters of private insurance and pension plans and funds”.

Insurance brokers are one of three classes of insurance dealers

contemplated by Royal Decree-Law 3/2020 (article 134). In turn, in the category of

insurance intermediaries include insurance agents and brokers

insurance (article 135).

On the other hand, in accordance with article 137 of R.D-Law 3/2020, mediators of

Insurance companies can enter into commercial contracts with “external collaborators” who

carry out distribution activities on behalf of said mediators but who do not

In no case will they have the status of insurance mediators. Article 137.2.

establishes that "External collaborators will develop their activity under the

management, regime of administrative, civil professional liability, and regime of

financial capacity of the mediator for whom they act.”

For the purposes of the GDPR and the LOPDGDD, article 203 of R.D-Law 3/2020 specifies that

insurance agents will have the status of data processors

insurance entity with which they have signed the Agency contract. And adds that

will have the status of treatment managers of insurance agents

external collaborators with whom they contract in the terms provided in the

Article 137 of R.D-Law 3/2020. Thus, article 203 of R.D-Law 3/2020, "Condition

responsible or in charge of the treatment", provides:

1. For the purposes provided in Organic Law 3/2018, of December 5, as well as

in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27

of April 2016 regarding the protection of natural persons in what

regarding the processing of personal data and the free circulation of these

data:

a) Insurance agents and bancassurance operators will have the

condition of managers of the treatment of the insurance company with which

have entered into the corresponding agency contract, under the terms

provided for in title I.

b) […]

c) The external collaborators referred to in article 137 will have the

status of managers

or insurance brokers

treatment

of agents

with whom they have entered into the corresponding commercial contract. In this

case, they may only process the data for the purposes provided in article 137.1.

2. In the case provided for in letter a) of section 1, in the agency contract

The points provided for in article 28.3 of the

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27

April 2016.

Similarly, in the case provided for in section 1.c) must include

in the commercial contract entered into with external collaborators the extremes

provided for in article 28.3 of Regulation (EU) 2016/679 of the Parliament

Council and Council, of April 27, 2016." (The underlining is ours)

Article 204 of R.D-law 3/2020 adds that "2. Insurance agents […]

They may only process the data of the interested parties in the terms and with the scope

arising from the insurance agency contract and always in the name and by

account of the insurance company with which they have entered into the contract."

The office where the events that are the subject of the claim took place, located at

XXXX, belongs to the exclusive insurance agent of the INSURER, CUSEGUR

2015 Insurance Agency, S.L., with NIF B86920824. Indeed, like the

INSURER has alleged, the employee of the agent's office is not an employee

yours, but of your treatment manager, the CUSEGUR agent. The agent, in this

case, he acted through his employee in the development of the distribution activity in

which the INSURER had established the means and purposes of the processing that

Were performed.

Moreover, the CUSEGUR agent affirms that he did not mediate in the insurance contract that the

claiming party had subscribed with the INSURER since 2020. In such a way that,

In the present case, CUSEGUR intervened only in the preparatory activity of the

contracting an automobile insurance policy with a third party, with whom the

claimant had entered into an earnest money contract for the sale of his vehicle, who

went to his office on XXXX. The agent acted in his capacity as person in charge of

treatment of the claimed INSURER, in accordance with article 203.1.a) of R.D-

Law 3/2020.

On the alleged infringement of article 5 of the GDPR

IV.

1.The INSURER is attributed a violation of article 5.1.f) of the GDPR regarding

to the principle of confidentiality.

Recital 39 of the GDPR states that "Personal data must be treated as a

in a manner that ensures adequate security and confidentiality of the data

personal information, including to prevent unauthorized access or use of such data and

of the equipment used in the treatment."

It is appropriate to mention, at this point, the Judgment of the Constitutional Court (STC)

292/2000, which in its Legal Foundation 7, regarding the content of the right

to the protection of personal data, says:

"[…] it turns out that the content of the fundamental right to data protection

consists of a power of disposal and control over the personal data that

empowers the person to decide which of those data to provide to a third party, be it

the State or an individual, or which can be collected by this third party, and which also allows

the individual to know who owns that personal data and for what, being able to oppose

to that possession or use. These powers of provision and control over the data

personal, which constitute part of the content of the fundamental right to

data protection are legally specified in the power to consent to the collection,

obtaining and accessing personal data, its subsequent storage and

treatment, as well as its use or possible uses, by a third party, be it the State or a

particular. And that right to consent to the knowledge and treatment, computerized or

no, of the personal data, requires as essential complements, for a

hand, the power to know at all times who has that personal data and

to what use he is putting them, and, on the other hand, the power to oppose that possession and

applications." (The underlining is ours)

2. It is proven in the file that the INSURER, through its

person in charge of treatment, the exclusive agent COSEGUR, provided the third party with a

document in which personal data of the claimant regarding her

personal identification, telephone contact, address and nationality, and referring to the

insurance policy on the vehicle that gave rise to the dispute at hand

and the claims that he had declared to the INSURANCE COMPANY during the validity of the

contract signed with her.

In its response to the request for information from the Sub-directorate of Inspection, the

INSURER denies that it had violated the right of the claimant in matters

of data protection and alleges that the third party had knowledge of the information

Well, some time before the events, on 08/27/2021, he had signed a contract with the claimant

deposit contract for the purchase of your vehicle. And he adds that, given that

had the vehicle in his possession before the events occurred, it is possible to think that

He agreed to the documentation that should appear in said vehicle. In this sense,

has become known as a result of the inspection actions carried out, which was the third

who delivered and removed the vehicle from the repair shop. Although it cannot be proven

the delivery date in the workshop is inferred to be 09/06/2021 because it was then

when the report for the vehicle's appraisal was opened.

However, it has not been proven that the third party had known with

prior to the facts, all the data concerning the claimant that was

included in the document to which you had access. To which it should be added that, for the

third party could legitimately access the data of the affected party, there must be a

legal basis for such treatment in accordance with article 6.1 of the GDPR.

The INSURER has declared regarding this matter that the business of its

insurance agent acted on the basis of the legitimate interest of the third party who, in his opinion,

was revealed by his status as future buyer and holder in that

time of the vehicle in dispute.

In view of what is alleged by the claimed party, and without prejudice to the outcome of the

instruction, it should be underlined that, in accordance with the principle of proactivity, article 5.2

of the GDPR, the INSURER should in such a case have deployed the diligence that

it was appropriate, given the particular circumstances that arose,

to certify that the treatment was based on the grounds of legality that were

invokes and have collected the necessary documentation to prove the concurrence of

that legal basis. In addition, the third party did not turn out to be the buyer of the vehicle because

According to information provided by the DGT, the vehicle referred to in this file was

transferred on 10/29/2021 to a person whose data does not match those of the

third.

3. Law 40/2015, of October 1, on the Legal Regime of the Public Sector (LRJSP)

provides in article 28.1 that "They may only be penalized for acts constituting

of administrative infraction natural and legal persons, [...] that result

responsible for them by way of fraud or negligence.”

Recital 74 of the GDPR says on this issue:

"The responsibility of the data controller must be established for

any processing of personal data carried out by himself or on his behalf. In

In particular, the person responsible must be obliged to apply timely and effective measures

and must be able to demonstrate the compliance of the processing activities with the

this Regulation, including the effectiveness of the measures. These measures must have

into account the nature, scope, context and purposes of the processing as well as the

risk to the rights and freedoms of natural persons.”

The Judgment of the National Court, Contentious-Administrative Chamber,

Section 1, of 04/13/2005 (Rec. 230/2003), after assuming that the

Strict liability is proscribed in our legal system and must be

always respect the principle of guilt -which is inferred from the Constitution, in

particular of the principles of legality and prohibition of excess, article 25 C.E., or

of the demands inherent to a Rule of Law-, says the following:

“In the present case, it is necessary to take into consideration […] that when there is a

specific duty of vigilance the fault is integrated by the simple breach of the

duty of vigilance, without requiring any further accreditation at the time of

Assess whether there has been a breach of the duty to keep secret. This criterion

results from judgments such as the one dated December 18, 2002 (appeal 1096/2000)

in a case very similar to the one that concerns us now and whose arguments are

perfectly transferable to the present case, according to which "Well, the conduct

that configures the administrative offense -article 44.2.e) of the Organic Law 5/1992-

requires the existence of guilt, which materializes, for what is now of interest, in the

simple breach of the duty to keep secret, a duty that is transgressed when

information is provided to third parties of the data that about the holder of an account

bank provides the appellant entity, (...) since the bank entity did not observe a

diligent conduct tending to safeguard the expressed duty of secrecy, and this

conduct is sufficient to consummate the infringement provided for in the aforementioned article. In

Consequently, this lack of diligence configures the guilty element of the

administrative offense and is attributable to the appellant". (The underlining is ours)

In this case, the element of guilt, necessary for the birth of the

disciplinary liability against the INSURER, is made up of the lack of

diligence shown by the claimed party in compliance with the principle of

confidentiality.

4. The violation of article 5.1.f) of the GDPR that is attributed to the person claimed in this

initiation agreement is typified in article 83.5.a) of the GDPR, which provides:

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

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

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

total annual global business volume 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 under articles 5, 6, 7 and 9;

[…]"

For the purposes of prescription of infringements, article 72 of the LOPDGDD, under the

under the heading "Infractions considered very serious", provides:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679,

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

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

following:

a) The processing of personal data in violation of the principles and guarantees

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

On the alleged infringement of article 32 of the GDPR

V

1. The INSURER is attributed a violation of article 32 of the GDPR, precept

which obliges the data controller to guarantee the security of the data and to

apply the technical and organizational measures that are appropriate to guarantee

a level of security adjusted to the risk involved in the treatment. The adequacy of the

level of security to the risk must be evaluated by the person in charge and reconsidered

periodically based on the results obtained taking into account for it -

among other factors - the risks that the treatment may present as

consequence of the unauthorized communication of said data.

The technical and organizational measures that must be applied are the pertinent

to respond to the existing risk, assessing for this purpose, among other factors, the state

of the technique, the application costs, the nature, scope, context and purposes

of the treatment and the risks of probability and seriousness for the rights and freedoms

of interested people.

Recital 83 of the GDPR says in this sense:

"(83) In order to maintain security and prevent processing from infringing the provisions of

this Regulation, the controller or processor must assess the risks

inherent to the treatment and apply measures to mitigate them, such as encryption. Are

measures must ensure an adequate level of security, including the

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and nature of the personal data to be

protect yourself. When assessing risk in relation to data security, considerations should be

take into account the risks arising from the processing of personal data,

such as the destruction, loss or accidental or unlawful alteration of personal data

transmitted, stored or processed in another way, or communication or access not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

The GDPR, unlike the previous regulations, particularly the Royal Decree

1720/2018, by which the Regulations for the development of the Organic Law were approved

15/1999, Protection of Personal Data (LOPOD), does not establish a

List of applicable security measures.

On the contrary, the GDPR incorporates the principle of proactive responsibility (article

5.2) by virtue of which it is incumbent on the controller to comply with the obligations imposed on him

the GDPR, in this case its article 32, as well as the obligation to be in good conditions

to certify its compliance.

Opinion 3/2010, of the Article 29 Working Group (GT29) -WP 173- issued

during the validity of Directive 95/46/EEC, repealed by the GDPR, but whose

reflections are applicable today, affirms that the "essence" of the

Proactive responsibility is the obligation of the data controller to apply

measures which, under normal circumstances, ensure that in the context of the

processing operations comply with data protection regulations

and in having available documents that demonstrate to the interested parties and the

Control authorities what measures have been adopted to achieve compliance

of data protection regulations.

As stated by the Legal Office of the AEPD (among others, reports 17/2019

and 64/2020) the GDPR has meant a paradigm shift when addressing the regulation of

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

of “proactive responsibility” (“accountability”) The statement of reasons for the

LOPDGDD says that "the greatest novelty presented by Regulation (EU) 2016/679 is

the evolution of a model based, fundamentally, on compliance control

to another that rests on the principle of active responsibility, which requires a prior

assessment by the person in charge or by the person in charge of the risk treatment that

could generate the processing of personal data for, from said

assessment, adopt the appropriate measures”

2. The documentation in the file proves that, dated 09/22/2021,

from an office of the exclusive agent of the claimed INSURER, CUSEGUR,

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

15/22

provided to the third party (who, in turn, had entered into a contract of

deposit for the purchase of the vehicle) a document with the name of the entity

insurance company -PELAYO MUTUA DE SEGUROS- and abundant information regarding

the policy ***POLIZA.1 subscribed with the claiming party.

The information contained in the document dealt with "Customer Data" -
name and two surnames of the claimant, NIF, mobile phone number, address and
nationality-, the "Policy data" -date of the policy, registration, make and model
of the vehicle-, and about the "Accidents" that were declared - four accidents of
which provided the identification number, the date on which it occurred and the date
in which it was declared. Among them, the last one, with reference number XXXXXXX,
occurred on 08/29/2021 and declared on 09/06/2021.
The existing documentation evidences the bankruptcy of the security measures that the
The claimed party, in its capacity as data controller, was obliged to
deploy because it is her responsibility to guarantee a level of security
appropriate to risk.
3. In relation to the essential element of guilt, we assume
reproduced the general considerations included in Fundament IV
preceding.
In the violation of article 32 of the GDPR that is attributed to the person claimed in this
initiation agreement the element of guilt is integrated by the lack of diligence
demonstrated in compliance with the obligation imposed by that precept of
establish and apply appropriate measures to ensure data security.
The sentence of the Supreme Court, Chamber of Contentious-
Administrative, Section 3, of 02/15/2022 (Rec. Cassation 7359/2020) that, in its
Third legal basis, "About security measures in terms of
data protection and legal persons", says:
"It is not enough to design the necessary technical and organizational means, it is also
necessary its correct implementation and its use in an appropriate way, so that
will also respond for the lack of diligence in its use, understood as a
reasonable diligence considering the circumstances of the case.

This distinction is also reflected both in the Regulation of the European Union 2016/679, of the Parliament and of the Council regarding the protection of natural persons regarding the processing of personal data and the free circulation of these data, as in LOPD 3/2018 of December 5, […] when differentiating as obligations and autonomous infractions between the lack of adoption of those measures technical and organizational that are appropriate to guarantee a level of security appropriate to the risk of treatment (art. 73 sections d, e and f) and the lack of due diligence in the use of technical and organizational measures implemented (art. 73.g).” (The underlining is ours)

4. The violation of article 32 of the GDPR that is attributed to the person claimed in this initiation agreement is typified in article 83.4.a) of the GDPR, which provides:

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

a) the obligations of the controller and the person in charge under articles 8, 11, 25 to 39, 42 and 43”.

For the purposes of prescription of infringements, article 73 of the LOPDGDD, under the under the heading "Infractions considered serious", provides the following:

"Based on what is established in article 83.4 of Regulation (EU) 2016/679,

are considered serious and will prescribe after two years the infractions that suppose a substantial violation of the articles mentioned therein and, in particular, the following:

[…]

f) The lack of adoption of those technical and organizational measures that result appropriate to guarantee a level of security appropriate to the risk of the treatment, in the terms required by article 32.1 of Regulation (EU) 2016/679

g) The breach, as a consequence of the lack of due diligence, of the technical and organizational measures that have been implemented as required by article 32.1 of Regulation (EU) 2016/679."

Penalty that could be imposed for violations of articles 5.1.f) and 32 of the GDPR

SAW

Article 70.1 of the LOPDGDD provides that they are subject to the sanctioning regime established in Regulation (EU) 2016/679 and in this organic law: "a) The responsible for the treatments."

The corrective powers attributed to the AEPD as control authority are detailed in Article 58.2 of the GDPR, sections a) to j), among which the precept includes the power to impose an administrative fine in accordance with article 83 of the GDPR (article 58.2. i).

Notwithstanding what results from the investigation, it is considered in the present case that it would be appropriate to impose on the INSURER individual sanctions of an administrative fine for the alleged violations of articles 32 and 5.1.f) of the GDPR.

Article 83 of the GDPR, "General conditions for the imposition of fines administrative", it says in its section 1 that the control authority will guarantee that the imposition of fines for the infringements of this Regulation indicated in the

sections 4, 5 and 6 comply, in each individual case, with the principles of effectiveness,

proportionality and dissuasiveness.

The principle of proportionality implies a correlation between the offense and the sanction,

with the prohibition of unnecessary or excessive measures, so that it must be

fit to achieve the ends that justify it. Article 83.2. of the GDPR determines the

technique to be followed to achieve that adequacy between the sanction and the infraction committed and

offers a list of criteria or factors that will be taken into account to graduate the

sanction.

Violations of the GDPR that may be incurred by those responsible and in charge

of the treatment are classified according to their nature in sections 4 to 6 of the

Article 83 of the GDPR.

Therefore, the GDPR foresees two categories of infringements according to article 83: the

regarding the infringements of section 4, which are punishable by a maximum fine of 10

million euros or 2% of the annual turnover of the company if the latter

is higher, and that of sections 5 and 6 of article 83, which is punishable by a fine

maximum of 20 million euros or 4% of the annual turnover of the

company, whichever is higher.

In relation to those sections of article 83 of the GDPR, the European Committee of

Data Protection comments in its Guidelines 4/2022, for the calculation of fines

administrative procedures under the GDPR, approved for public consultation on 05/12/2022,

(heading 49): "With this distinction, the legislator provided a first indication of

the seriousness of the infringement in an abstract sense. The more serious the

infraction, the greater the fine."

1.-Determination of the amount of the penalty that would be imposed on the party

claimed for the violation of article 5.1.f) of the GDPR.

At this stage of the procedure, in view of the documentation in the

file, and, in any case, without prejudice to the result of the investigation, the

the following aggravating factors described in article 83.2 of the GDPR:

- Circumstance of article 83.2.b) of the GDPR, "intentionality or negligence in the

infringement".

The claimed party has acted with a serious lack of diligence in the treatment

carried out in the development of the insurance distribution activity of its own.

Regarding the degree of diligence that the person in charge is obliged to display in the

compliance with data protection regulations, it is worth mentioning the SAN of 10/17/2007

(Rec. 63/2006) in which it mentions that "[...] the Supreme Court has been understanding

that recklessness exists whenever a legal duty of care is neglected, it is

that is, when the offender does not behave with the required diligence. And in the valuation

of the degree of diligence, the professionalism or not of the

subject, [...] (emphasis added)

The claimant was a client of the INSURANCE company when the events occurred.

facts, so that it was obliged to maintain the confidentiality of their data

personal information that it was only empowered to process for the purposes related to the

execution of the contract.

- Circumstance of article 83.2. k) GDPR, in relation to article 76.2.b)

LOPDGDD:

"The linking of the offender's activity with the performance of data processing

personal."

Considering the circumstances that concur, the sanction of a fine that could be

impose on the INSURER for the alleged violation of article 5.1.f) of the GDPR,

classified in article 83.5, which provides for a maximum penalty of €20,000,000, would be

€50,000 (fifty thousand euros).

2. Determination of the amount of the sanction that would proceed to be imposed on the party

claimed for the infringement of article 32 of the GDPR:

At this stage of the procedure, in view of the documentation in the

file, and, in any case, without prejudice to the result of the investigation, the

the following aggravating factors described in article 83.2 of the GDPR:

-Circumstance of article 83.2.g) "the categories of personal data

affected by the infringement

Regarding this circumstance, Directives 4/2022 say (heading 58) that "the

GDPR clearly outlines the types of data that deserve special protection and,

therefore, a stricter response in terms of fines. This is referred to as

minimum, to the types of data contemplated in articles 9 and 10 of the GDPR, and to the

data that do not fall within the scope of these articles whose dissemination causes

immediate damage or hardship to the data subject (for example, location data,

data on private communications, national identification numbers). In

In general, the more of these categories of data are processed or the more sensitive the

data, the more serious the infraction."

And he adds: "In addition, the amount of data relating to each interested party is relevant,

taking into account that the intrusion of the right to privacy and the protection of

personal data increases with the amount of data relating to each data subject."

It has been accredited in the file that the INSURER, through the agent

exclusive, provided the third party with a document containing a multitude of data

personal information of the complaining party. Among the identifying data, your ID in addition to the

name and surname, address and telephone number among others. but also those

related to the policy subscribed, the claims declared or the way in which you paid

the insurance premium.

- Circumstance of article 83.2. k) GDPR, in relation to article 76.2.b)

LOPDGDD:

"The linking of the offender's activity with the performance of data processing

personal."

Considering the circumstances that concur, the sanction of a fine that could be

impose on the INSURER for the alleged violation of article 32 of the GDPR,

classified in article 83.4, which provides for a maximum penalty of €10,000,000, would be

€20,000 (twenty thousand euros).

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

Spanish Data Protection,

HE REMEMBERS:

FIRST: INITIATE SANCTION PROCEDURE against PELAYO, MUTUA DE

INSURANCE AND REINSURANCE AT FIXED PREMIUM, with NIF G28031466:

1. For an alleged violation of article 5.1.f) of the GDPR, typified in article

83.5.a) of the GDPR.

2. For an alleged violation of article 32 of the GDPR, typified in article 83.4.a)

of the GDPR.

SECOND: APPOINT instructor to F.F.F. and secretary to G.G.G., stating that

may be challenged, where appropriate, in accordance with the provisions of articles 23 and 24

of Law 40/2015, of October 1, on the Legal Regime of the Public Sector (LRJSP).

THIRD: INCORPORATE into the disciplinary file, for evidentiary purposes, the

claim filed by the claimant and its attached documentation, as well as

the documents obtained and generated by the Sub-directorate General of Inspection of

Data in the actions prior to the start of this sanctioning procedure.

FOURTH: THAT, for the purposes set forth in article 64.2 b) of the LPACAP, the sanction

that could correspond would be an administrative fine:

1. For violation of article 5.1.f) of the GDPR of €50,000 (fifty thousand euros)

2. For the violation of article 32 of the GDPR, €20,000 (twenty thousand euros)

The total amount of the fines corresponding to the two infractions amounts to

€70,000 (seventy thousand euros).

FIFTH: NOTIFY this agreement to PELAYO MUTUA DE SEGUROS AND

FIXED PREMIUM REINSURANCE, with NIF G28031466, granting a period of

audience of ten business days to formulate the allegations and present the

tests you deem appropriate. In your pleadings you must provide your

NIF and the number of the procedure that appears in the heading of this

document.

If, within the stipulated period, he does not make allegations to this initial agreement, the same

may be considered a resolution proposal, as established in article

64.2.f) of the LPACAP.

In accordance with the provisions of article 85 of the LPACAP, you may recognize your responsibility within the period granted for the formulation of allegations to the present initiation agreement, which will entail a reduction of 20% of the sanction that should be imposed in this proceeding. With the application of this reduction, the sanction would be established at €56,000 (fifty-six thousand euros), resolving the procedure with the imposition of this sanction.

In the same way, 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 €56,000 (fifty-six thousand euros) and its payment will imply the termination of the procedure, without prejudice to the imposition of the corresponding measures.

The reduction for the voluntary payment of the penalty is cumulative to the corresponding apply for acknowledgment of responsibility, provided that this acknowledgment of the responsibility is revealed within the period granted to formulate allegations at the opening of the procedure. In this case, if it were appropriate to apply both reductions, the amount of the sanction would be established at €42,000 (forty-two a thousand euros).

In any case, the effectiveness of any of the two aforementioned reductions will be conditioned to the withdrawal or resignation of any action or appeal via administrative against the sanction.

If you choose to proceed with the voluntary payment of any of the amounts indicated previously, €56,000 or €42,000, you must make it effective by depositing it in the account number IBAN: ES00 0000 0000 0000 0000 0000 (BIC/SWIFT Code: XXXXXXXXXXXX) opened in the name of the Spanish Agency for Data Protection in the banking entity CAIXABANK, S.A., indicating in the concept the number of reference of the procedure that appears in the heading of this document and the cause of reduction of the amount to which it receives.

Likewise, you must send proof of income to the General Subdirectorate of Inspection to continue with the procedure in accordance with the quantity entered.

The procedure will have a maximum duration of nine months from the date of the initiation agreement or, where appropriate, of the draft initiation agreement. After this period, its expiration will occur and, consequently, the file of actions, 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, as regards successively, the notifications that are sent to you will be made exclusively in a electronically, through the Unique Authorized Electronic Address (dehu.redsara.es) and the Electronic Notification Service (notifications.060.es), and that, if you do not access their rejection will be recorded in the file, considering the process completed and following the procedure. You are informed that you can identify before this Agency an email address to receive the notice of making available to the notifications and that failure to practice this notice will not prevent the notification be considered fully valid.

Finally, it is noted that in accordance with the provisions of article 112.1 of the LPACAP, there is no administrative appeal against this act.

Mar Spain Marti

Director of the Spanish Data Protection Agency

>>

SECOND: On March 23, 2023, the claimed party has proceeded to pay of the sanction in the amount of 42,000 euros making use of the two reductions provided for in the initiation Agreement transcribed above, which implies the recognition 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 appeal via against the sanction and acknowledgment of responsibility in relation to the facts referred to in the Commencement Agreement.

FUNDAMENTALS OF LAW

Yo

Competence

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), 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 Data Protection Agency will be governed by the provisions

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

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures."

II

Termination of the procedure

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

Common for Public Administrations (hereinafter, LPACAP), under the heading

"Termination in disciplinary proceedings" provides the following:

"1. Initiated a disciplinary procedure, if the offender acknowledges his responsibility,

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

2. When the sanction has only a pecuniary 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 presumed perpetrator, in

any moment 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 offence.

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

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

20% of the amount of the proposed penalty, these being cumulative among themselves.

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 resource against the sanction.

The percentage reduction provided for in this section may be increased

according to regulations."

According to what has been stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARE the termination of procedure EXP202201254, in

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

SECOND: NOTIFY this resolution to PELAYO MUTUA DE SEGUROS AND

FIXED PREMIUM REINSURANCE.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process as prescribed by

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

Common of Public Administrations, interested parties may file an appeal

administrative litigation before the Administrative Litigation 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 for in article 46.1 of the

referred Law.

Mar Spain Marti

Director of the Spanish Data Protection Agency

936-040822

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es