 File No.: PS/00413/2021

- RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: The CIVIL GUARD - POST OF TOTANA sends, on date

06/18/2020, Minutes-Complaint-Inspection and Request for procedure for infringement of the

regulations on data protection, noting that on 04/22/2020 they appear in person at the

dependencies of the body D. A.A.A. (hereinafter the complaining party) together with a

third, delivery person for the company General Logistics Systems Spain, S.A. (in

successive GLS) The reasons on which the claim is based are the following: that the

employee of the company intended to give him a mobile phone sent by the

company ORANGE ESPAGNE S.A.U. (hereinafter the defendant), and that the company

mentioned to deliver the packages to their recipients, is imposing

as a necessary condition to take a photograph of the front and back of your ID. He

company employee takes it with his mobile terminal at the time of delivery.

Subsequently, the image obtained is transferred to the company that sent the package.

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), with reference number E/05859/2020, transfer of

said claim to the defendant and to other entities with which the claim was related.

delivery of the package, so that they proceed to its analysis and inform this Agency

within a month, of the actions carried out to adapt to the requirements

provided for in the data protection regulations.

GLS, whose delivery person was to deliver the mobile phone, alleges the following:

Despite not having the essential data to identify the shipments, they believe
have identified the reported delivery service, which they go on to explain. HE
called IdentService, and has its origin in the requirement of its clients so that
the identity documents of the recipients are photographed, thus providing a
greater security that the package has actually been delivered to the addressee and
not to any person who could live in the same address as this.
The procedure was implemented in September 2018 to comply with the
requirements of your ICP client. In addition to the corresponding manager contract,
signs a special addendum in which GLS assumes the role of representative under the
orders of the principal for the collection of the photographs of the documents of
identity. The contract is provided as the addendum, signed with ICP.
C / Jorge Juan, 6
28001 – Madrid
www.aepd.es
sedeagpd.gob.es
2/21
Customers who decide to require this photograph record it in the system that
provides GLS in the form of a special attribute associated with the delivery of the shipment that
wish. The necessary information travels to the device of the delivery person who performs the
delivery (full name of the recipient and ID. At the time of delivery, if
name or ID do not match what is indicated, the delivery cannot be made. Yeah
match, the delivery application allows you to take a photo of the front and back of the
DNI, so that it can be delivered. The collected data is transmitted by channel
encryption to the GLS system (they are not saved on the driver's delivery device,
with which he cannot consult the images) and they remain stored on a server
internal property of GLS, separated from the rest of the images (signatures and stamp photos).

Only a maintenance technician has access to that server. through the

ERP module of the computer system, customers can access the photos

of the shipment that they have marked to carry out of this signature, through a link (not

can consult photographs of DNIs indiscriminately). the pictures are

stored and processed for customer consultation or to respond to possible

claims about shipping incidents, for 1 year (for the purposes of

extrajudicial claims) and 4 years (as it is considered a commercial document - art.

66 LGT 58/2003). The photographs also cannot be seen by the delivery person from

your device.

They also have another service, "Online DNI validation service" (consumed

only by this client, ICP), in which in real time it is transmitted to the

ICP the data of full name, DNI and images of the front and back of the DNI, and

They wait for a response from him. If the system returns a KO (negative response), the

prevent delivery; otherwise allowing (positive response or lack of

answer).

The procedure established for the delivery of the package provides that it must be

request the interested party to allow them to photograph the DNI, as it is a mandatory requirement

imposed by the customer for delivery. The recipient is free to do so, but it is

informed of the consequences of not being able to verify the

identity. The basis of legitimacy is not the consent but the execution of the

contract with your client. It will be this, the supplier of the product, who will inform the

recipient of the procedure and request their consent, if this is the basis

legitimizer used".

THIRD: On 11/04/2020, the Director of the AEPD agrees the admission to

claim processing.

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

documents provided by the claimant, the Sub-directorate General of Inspection of

Data proceeded to carry out previous investigation actions for the

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

granted to control authorities in article 58.1 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 Law

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

digital rights (hereinafter LOPDGDD).

On 09/02/2020, this Agency received a written statement stating

the following relevant aspects:

- The defendant makes shipments by itself or through subcontracted companies.

you give.

- The claimed has a delivery method called Identservice (DNI + photo)

which has its origin in the requirement of the ICP client to provide greater security.

that the package has been delivered to the addressee.

- If a client requests the Identservice service, once the shipment reaches the company

collaborator in charge of its delivery at the destination, the delivery person asks the recipient

the full name and the DNI and if these coincide with the data in the term-

delivery man, take a photo of both sides of the DNI. In case the data

full name or ID do not match those that appear in the deliveryman's terminal,

delivery and photo is not done. They add that the data collected is transmitted from

encrypted form to their systems, not saving the recipient's data or the photos received.

recently taken at the dealer's terminal, so he cannot consult them. Is-

All data is stored on a specific server for this function owned by the

claimed company and to which only one person has access for maintenance tasks.

I lie. In addition, the images must be taken with the application of the claimed that

is in charge of sending them to the mentioned server without storing them in the terminal of the re-

splitter, not admitting this application that can be taken with the mobile camera and

pass them to the application for transmission. It should be noted that in the event that the

client is ICP, the photograph of the DNI is sent through the claim servers.

gives to ICP systems.

- However, the data can be accessed from the ERP system (Project Planner).

Business Resources that allows the exchange of data between different areas)

of the claimed The person responsible for the shipment, the person responsible for

of delivery, and the customer responsible for shipping. The images are treated only

by its clients or to respond to possible claims of incidents of

shipment and only those data that correspond to the shipment of each client.

- The data is kept for one year for the purposes of extrajudicial claims and

for the purposes of proof of delivery, for four years as it is considered a mercantile document.

cantil.

- They indicate that their responsibility is that of the person in charge of the treatment, being the person responsible

saber of this, the client who requested this type of verification in the delivery. Therefore,

the basis of legitimation is not the consent of the sender, but the execution of the

contract with your client, being the latter the one who reports this treatment and collects the

sentiment of the recipient for the treatment.

C / Jorge Juan, 6

28001 – Madrid

And attach the following documents:

- Service contract with ICP in which the claimed entity appears as manager

of treatment, being the person in charge of this treatment, ICP.

- Addendum service contract with ICP (DNI + photo) in which the claimed appears

as agent

- Descriptive poster of the three types of sender identification

Requested by this Agency, the contracts with the clients corresponding to the

Routes sent to claimants, dated 10/28/2020, are received at this Agency

three writings, stating:

1.- Regarding the shipment made to the claimant of an ORANGE product through

of the ICP entity, it had requested the validation modality with a photo of DNI.

They provide document of expedition nº ***EXPEDIENTE.1. It shows the requirement

compliance with this type of validation requested by ICP.

On 11/04/2020, in procedure E/05859/2020, the Spanish Agency for

Data Protection agreed to carry out these investigative actions

in relation to the claims submitted by the claimants.

- Regarding the claim presented by the claimant (through the Guardia Ci-

vile) the defendant is asked for the basis of legitimacy to obtain a photograph.

ID card, the recipient's consent and the information provided to this envelope

the treatment.

On 02/19/2021, this Agency received a written response manifesting

tando:

- That they understand that the basis of legitimation resides in the need to execute the

contract to which both the claimant and the respondent are parties.

- That prior to the delivery of the product sent by the claimant with validation

tion by taking a photograph of the claimant's DNI, the claimant sent a co-

email to the claimant informing him that for security reasons the document

identification document with which the product was contracted could be digitized at the same time.

delivery time. Likewise, the conditions of the deliveries of the orders that

makes the claim to its clients, details can be found on the official website, at

through the following link:

https://ayuda.orange.es/particulares/movil/mi-movil/mi-pedido/1101-donde-recojo-mi-

order-and-what-documentation-do I need?

utm_source=orange&utm_medium=SMS&utm_term=smsAltaPedido

And attach the following documents:

- Contract signed by the claimant and claimed dated 01/18/2020 and "Annex

of Privacy" dated 12/30/2018 signed by the claimant

- Content of the email sent to the claimant.

It has been verified that the web link they provide contains the requirement that

the identification document with which the product was contracted will be typed

ized at the time of delivery.

FIFTH: On 09/17/2021, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged in-

fraction of 5.1.c), typified in article 83.5.a) of the GDPR.

SIXTH: Notified of the initiation agreement, the claimant on 09/23/2021 requested extension of the term to present allegations; period that was granted by means of you written from the instructor of 09/24/2021.

The defendant by writing of 10/11/2021 presented a written statement of manifest summarizing the following: that a treatment of the image of the DNI is carried out lawful, as long as it pursues a legitimate interest; previously the AEPD has come penalizing the defendant for the absence of said treatment, considering it a lack of diligence in compliance with the obligations derived from the regulations data protection; that the National Court, in its Judgments of March 8 of 2018 and May 5, 2021, which indicates that the person responsible for the treatment must keep documentary evidence of compliance with their obligations in protection of data, such as verification of the identity of the interested party to whom a product contracted at a distance; that the defendant is faced with a clear contradiction and legal uncertainty; that secondarily, in the event that it is not taken into account taking into account the grounds supported by the defendant, it is requested that the account the extenuating circumstances and, consequently, complete the procedure through a warning and, ultimately, if he considers that the impo- sanction, moderate or modulate its proposal included in the Initiation Agreement cio of Procedure. .

SEVENTH: On 12/20/2021 a test practice period began, according to giving the following

Deem reproduced for evidentiary purposes the claim filed by the re- claimant and his documentation, the documents obtained and generated by the Inspection services that are part of file E/05859/2020.

Deem reproduced for evidentiary purposes, the allegations to the initiation agreement submitted by the defendant.

Request both the claimant and the company Information Control and Planning

tion that provide a copy of the collaboration contract signed between them, to

the

services.

benefit

of

On 12/29/2021, the defendant responded to the test carried out whose

content works in the file.

EIGHTH: On 04/07/2022, a Resolution Proposal was issued in the sense of

that the Director of the Spanish Data Protection Agency sanction the

claimed for violation of article 5.1.c), typified in article 83.5.a) of the

GDPR, of the aforementioned Regulation a fine of €100,000 (one hundred thousand euros). is accompanied

Annex with the documents that make up the administrative file.

The defendant entity, after requesting an extension of the term to present allegations to the

proposal, presents, on 05/05/2022, a brief of allegations in which it reiterates the

already raised previously. Indicates that reference is made to other claims that

They are not related to the facts that are the subject of this proceeding.

They point out that the account of the facts included in the First Background is not accurate.

of the Resolution Proposal: the ID photo is not taken with the terminal camera

end of delivery, but with a specific application within the terminal, which does not allow

access the image and not store it on the device.

At the time the photograph is taken, it is verified that the name and ID
that is contained in the delivery terminal corresponds to the ID and identifying name
fallen by the application. The application only allows photography if the
data correspond, so that, if there are data different from those provided,
ron at the time of contracting the product by the interested party, the photo is not taken.
graph. The ultimate goal is to guarantee that the terminal is delivered to the person who has it.
hired. That is, after the identification of the contracting party, carried out at the time of
remote contracting, the identification of the receiver of the terminal is carried out, which has
to be the same person.
Only in the event that the data does correspond, the distribution application
Allows you to take a photo of the front and back of the ID. The collected data is transmitted
sent by encrypted channel to the GLS system and are stored on an internal server.
suit, separated from the rest of the images. Only a maintenance technician has
access to that server. Through the ERP module of the computer system, Orange
You can access (only) the photograph of the shipment, through a link, to the me-
For the purposes of being able to verify that the process has been carried out correctly.
The purpose of the treatment of the images of the DNI of the interested party is none other than
certify, subsequently and if necessary, having deployed the diligence
required by verifying the identity of the person to whom the product is delivered
hired.
The data processing now questioned in the present sanctioning procedure
was implemented by Orange as a reinforcing security measure against ca-
fraud attempts and identity theft that were taking place
in the year 2020 in connection with the receipt of home deliveries.
Now, it is intended to penalize this party for displaying an excessive level of diligence.
vo in the identification of its clients, despite the fact that there is no legal precept, resolution or

jurisprudence that supports such an accusation, nor does it regulate how to identify

a data controller to their clients in contexts such as those analysed.

The AEPD considers that there are clear indications that article 5 of the

RGPD when imposing as a condition in the delivery to take a photograph of the front and

back of ID. I would like this part to recall that it is precisely this article 5 of the

RGPD which indicates, in its section 2: "The controller will be responsible for

able to demonstrate compliance with the provisions of paragraph 1 ('responsibility').

proactive responsibility»)".

If Orange does not have supporting evidence that it has delivered to the

contracting person, what could he do in the event that he claimed not to have received

did you buy the product? And in the event that the product, a mobile terminal, had data?

of a personal nature, for example, because it is a terminal from the service of

repair or technician? Would the Agency consider that in such a case it would also be

excessive to take a picture of the ID? What if the delivery package contained a card?

ta sim? Note at this point that the delivery men and courier companies do not know

They do not know the contents of the packages.

PROVEN FACTS

FIRST. On 06/18/2020 it has entry in the AEPD, Record-Complaint-Inspection and Pe-

revocation of proceedings for infringement of the regulations on data protection re-

submitted by the defendant stating that on 04/22/2020 they appeared at the

dences of the body D. A.A.A. together with a third party, a delivery man from the company General

Logistics Systems Spain, S.A. (hereinafter GLS) stating that the employee

of the company intended to deliver a mobile phone sent by the claimant

and that the aforementioned company, to deliver the packages to their desti-

natarios, is imposing as a necessary condition to take a photograph of the an-

front and back of your ID that the company employee takes with his terminal

mobile at the time of delivery. Subsequently, the image obtained is transferred to

the company that sent the package.

SECOND. The defendant in writing of 02/19/2021 has stated that "the legitimate

tion of this company for the treatment of personal data of Mr. A.A.A. resi-

of the need to execute the contract of which both the subscriber and Orange

are part, and which was signed on 01/20/2020, in accordance with the provisions of

article 6.1.b) of the GDPR"

THIRD. Contributed Contract for Private Clients mobile communications

signed between the claimant and the defendant on 01/20/2020.

ROOM. There is an email provided in which the claimant was informed

that, at the time of collecting the order, you should have your

Valid national identity document with which you contracted the services with the ci-

mercantile tada. Likewise, it was reported that, for security reasons, said document

This documentation could be required by the delivery person who delivered the order to your address.

cilium.

FIFTH. The defendant states that on his website, through the link

https://ayuda.orange.es/particulares/movil/mi-movil/mi-pedido/1101-donde-recojo-mi-

order-and-what-documentation do I need?

utm_source=orange&utm_medium=SMS&utm_term=smsAltaPedido, are also listed

the conditions for the delivery of the orders made by the defendant to his clients.

tes: Where do I pick up my order and what documentation do I need? Where can I pick up

did you get my order?

SIXTH. There is a document provided called "Privacy Annex", through

of which express consent is requested to carry out personal data processing.

personnel that are excluded from the purpose of executing the signed contract and are informed

of the purposes of the processing of personal data, as well as the categories

gories of data processed, in compliance with article 13 of the GDPR. The document is

is signed by the claimant.

SEVENTH. The defendant and ICP entered into a contract in Pozuelo de Alarcón (Madrid)

of provision of services whose purpose is the provision of mercantile deposit services.

cantil (storage of material of your business, commercial, promotional, technical

and network), logistics services (handling, assembly of the Goods, loading and

unloading of the same, transport of divided merchandise and its distribution, as well as

as the computer support of the operations carried out) all in accordance with

the agreed scope, prices and terms.

By virtue of this contract, ICP has the status of Treatment Manager;

It also contains a data protection clause, establishing that the person in charge

will carry out the processing of personal data necessary for the correct provision of

tion of the services object of the contract. The types of personal data that it will process in

under this contract are identifying data (name and surname, NIF/DNI).

EIGHTH. Confidentiality agreement and access to personal data is provided.

on behalf of third parties for service providers held in Madrid on

01/14/2018 between ICP, responsible for the treatment, and GLS, in charge of the treatment.

to, whose purpose is the processing of personal data necessary for the provision of the

messaging service (storage and custody of data).

NINETH. The Annex provides the contracting of the IdentService service (DNI +

foto) for clients of the latter, a complementary service to that of transport consisting

in the Identification of the Holder of the receipt of shipments of merchandise re-

wanted by the sending company. Its clauses state the following:

FIRST. The purpose of this Annex is the statement of the requirement of the

provision of the delivery service called IdentService (DNI + photo) whose con-

concept is expressed below.

SECOND. The IdentService (DNI + photo) consists in that, once the en-

charge for the provision of parcel delivery service, at the time

that delivery is made to the final recipient; the delivery man or messenger

asks him for his DNI to carry out the comparison and coincidence of the identity between the subject

subject to whom the package will be delivered and the subject indicated by the Client

of GLS to whom it must be carried out, having to reliably accredit said

identity to the company that sends the package.

THIRD. The DNI that the recipient must show must be the original document,

without a photocopy of it being valid, except in cases in which it is accredited

the original complaint before the Police stating the theft or loss of the same.

ROOM. The messenger or delivery man, at the time of delivery of the merchandise

will take a photograph of the DNI, in order to provide it together with the POD (Test
Delivery basis) to the Customer and certify that there is a correct correlation between
identity of the addressee and the person indicated by the Client of the subject to carry out the
delivery, having to send both documents to the Client that requires said service.
FIFTH. The Client, manifests with the signature of this Annex I, his agreement
regarding the request that the delivery man or messenger take the Photo of the DNI to the
recipient of the package, which, in case of refusing to show it, will not
the goods will be delivered.
SIXTH. The Client, who requires the IdentService service (DNI + photo) from GLS or its Network
Agency, assumes responsibility for as many claims as may be raised by the
recipients in this regard or as derived from this requirement, when acting
GLS as a mere representative of the Client, being the latter the one who requires and demands said
identity check action.
The Client is responsible for the treatment given to the photograph of the DNI of the
recipient and exempting GLS from any liability that may arise from the
practice of the service requested IdentService (DNI + photo), committing the latter
to the adequacy of its protocols to what is established by the General Regulation of
Data Protection 2016/679 of April 27, 2016 and other regulations in force in
The matter.
FUNDAMENTALS 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 au-
control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the Law
Organic 3/2018, of December 5, 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

Data processed by the Spanish Data Protection Agency will be governed by the dis-

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

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

subsidiary character, by the general rules on administrative procedures

you."

II

The denounced facts materialize in that the claimed company, when making

delivery of packages to their recipients through courier companies,

imposes as a necessary condition for the reception the taking of a photograph to the

front and back of your ID. The company employee takes it with his terminal

mobile at the time of delivery. Subsequently, the image obtained is transferred to the

company that sent the package.

Article 58 of the GDPR, Powers, states:

"2. Each supervisory authority will have all the following powers:

corrections indicated below:

(…)

i) impose an administrative fine in accordance with article 83, in addition to or instead of

from the measures mentioned in this paragraph, depending on the circumstances.

stances of each particular case;

(…)”

Article 5, Principles relating to processing, of the GDPR establishes that:

"1. Personal data will be:

(…)

c) adequate, pertinent and limited to what is necessary in relation to the purposes

for those who are processed ("data minimization");

(…)

II

1. The documentation in the file offers clear indications that

the defendant violated article 5 of the RGPD, principles related to treatment, by im-

put as a condition in the delivery of the product to take a photograph of the front and

back of the DNI; photograph that is obtained through the application included in the ter-

Mobile terminal of the delivery person of the company that makes the delivery and whose image is post-

subsequently transferred and consulted by the company sending the package.

Article 5 of the GDPR refers to the general principles for the treatment

of data. In its section c) reference is made to the principle of data minimization,

indicating that the data must be “adequate, pertinent and limited to what is necessary

in relation to the purposes for which they are processed”.

From the norm we can deduce that only personal data can be collected

that are going to be treated, that is, those that are strictly necessary

for the treatment; that they can only be collected when they are going to be treated and that

They may only be used for the purpose for which they were collected, but not with

no other goal.

In this same sense, Recital 39 states that:

(39) All processing of personal data must be lawful and fair. For the per-

physical persons it must be completely clear that they are collecting, using, con-
accessing or otherwise processing personal data that concerns them, as well as the
extent to which said data is or will be processed. The principle of transparency requires
that all information and communication related to the processing of said data is easy-
mind accessible and easy to understand, and that simple and clear language is used. Saying
principle refers in particular to the information of data subjects on the identity
of the person responsible for the treatment and the purposes thereof and the information added to
guarantee a fair and transparent treatment with respect to the natural persons affected
and your right to obtain confirmation and communication of personal data
that concern them that are subject to treatment. Natural persons must have
knowledge of the risks, standards, safeguards and rights related to the
processing of personal data as well as how to enforce your rights in
relation to treatment. In particular, the specific purposes of the treatment of the
personal data must be explicit and legitimate, and must be determined at the moment
of your collection. Personal data must be adequate, relevant and limited
what is necessary for the purposes for which they are processed. This requires, in particular,
ensure that their retention period is limited to a strict minimum. The personal data
personal data should only be treated if the purpose of the treatment cannot be reasonably achieved
probably by other means. To ensure that personal data is not retained
longer than necessary, the data controller must set deadlines for
their deletion or periodic review. All reasonable steps must be taken to
ensure that inaccurate personal data is rectified or deleted. The

Personal data must be processed in a way that guarantees security and confidentiality.

appropriate characterization of personal data, including to prevent unauthorized access or use

authorities of said data and the equipment used in the treatment (underlining is

of the AEPD).

Examining the documentation, it can be deduced that there are other procedures

delivery of products through which the identity of its destination can be verified.

notary, verifying that it is the person to whom it is addressed, without it being necessary to photograph

graph your ID through the application contained in the mobile of the company's delivery man

distribution company and accredit its delivery to the person in charge. The treatment of the images

ID card is excessive for the purpose of verifying and determining that the destination

The party to whom the goods are delivered is the same person as the person who entered into the

contract.

Article 5.1.c) enshrines the principle of data minimization and assumes that

The processing of personal data must be adjusted and proportional to the purpose for which

which it is addressed, clearly determining the purposes for which the data is collected and processed

the data, and the treatment of those that are excessive or

proceed to their deletion.

Likewise, the relevance in the treatment of the data must be produced both

in the field of collection as well as in the subsequent treatment carried out on the same

mos.

Regarding whether the procedure adopted by the defendant is necessary

to meet that need or if it is essential to meet that need,

It should be noted that its purpose, as repeatedly stated by the re-

claimed is due to the fact that it provides greater security that the product is effective.

delivered to the addressee, who is the same person who signed the contract, making

do proof that delivery is made to the person you actually hired; although to

To this we must add the fight against fraud in this type of product and its appearance economical since it must not be forgotten that these deliveries in the so-called retail sale has had and has a direct relationship with fraudulent activities, which requires reasonable diligence on the part of this type of company at the time of the treatment by implementing appropriate measures, verifying through documentation the identity of the person providing the data is pertinent, in order to avoid these behaviours.

In this sense, Recital 47 pronounces itself when it states that "The treatment storage of personal data strictly necessary for the prevention of Fraud also constitutes a legitimate interest of the data controller that in question".

However, the procedure used by the respondent is relevant to when assessing the interference in the fundamental right of data protection and the need to achieve the desired goal. It should be noted that the GDPR limits the use o treatment of data due to necessity and not due to excess thereof; that is to say, Personal data must be adequate, necessary, pertinent and limited. two to the need for which they were collected.

Previously, the Constitutional Court jurisprudence has established that, if the objective can be achieved without carrying out data processing, the same they should not be treated.

On the other hand, said limitation to what is necessary must be evaluated both from a quantitative point of view (volume of data processed) and qualitative (category of

processed data). In this same sense, Recital 39 points out when it states

that "…This requires, in particular, guaranteeing that their plan is limited to a strict minimum.

conservation zone. Personal data should only be processed if the purpose of the processing

performance could not reasonably be accomplished by other means..."

2. The defendant alleges that the data that was collected at the time of the

contracting the product were the DNI and the name of the interested party, which are the same

We provide data that is subsequently subject to verification at the time of delivery,

that are necessary to fulfill the pursued purpose.

However, such an allegation cannot be accepted, since access to the image

gene of the DNI, photographing both the back and the front of it, and its treatment

for the purpose of delivering a product through the mobile terminal of the re-

from the distribution company, is considered excessive and not limited to what is necessary

in relation to the purposes for which they are processed.

It should be noted that the DNI contains not only the name and surname, its number

and the recipient's photograph, but also incorporates many other data: signature, address,

place and date of birth, access code to the information contained therein,

issue date, validity date, alphanumeric code, issuing team and official

na, etc., completely additional data that is neither adequate nor pertinent nor

limited for the purpose of delivering the merchandise and that to prove that the

The person who collects the product is the owner who provided the data at the time of purchase.

contracting, other means that are less harmful and aggressive must be used

for people's privacy.

The foregoing, regardless of whether the image of the DNI, as stated by the

claimed cannot be kept by the dealer and be transmitted through

encrypted file to the logistics company system, being stored on its internal server.

external, where only a technician assigned to its maintenance has access to

said server and through the ERP query module of the computer system, the claimant

mado can access the collected photo.

Therefore, the treatment does not correspond to what is indicated in the Consideration

recital 39, nor in article 5.1.c) that state that the data must be “adequate,

pertinent and limited to what is necessary" for the purpose pursued.

That diligence that the defendant preaches must be deployed at the moment

contracting, adopting the necessary precautions and guarantees to identify

unequivocally certify the contracting party.

Therefore, if the recruitment is done correctly there can be no difficulty

any to provide proof that the recipient of the product is really the one who

entered into the contract and to whom the product is delivered.

3. The defendant alleges that the AEPD intends to qualify as constituting in-

fraction a treatment whose absence has been previously sanctioned by the AEPD.

However, such a statement is neither acceptable nor admissible; the claimed

must require at the time of contracting the product, the identification of the user,

As on the other hand, it has been established by the sentences and in the procedure

disciplinary measure to which he alludes in his writing.

Of course, it has nothing to do with the matter that the reference to the

Recital 64 of the GDPR to which the defendant refers, like those other

subsequent references to the right of access of the interested party regulated in article 15

of the legal text.

It is at the time of signing the contract that the treatment of the document

The identification of the interested party is considered necessary so that the defendant can

certify that the person with whom they contract is who they really say they are and, therefore,

therefore, which would accredit an adequate level of diligence.

And this moment should not be confused with the delivery of the product to your

addressee transferring that required diligence to prove that the personality

of the contracting party was who they claimed to be by providing the documentation

opportunely to a later moment, that of the delivery of the product to its addressee.

This has been indicated by the AEPD itself, in its resolution of 06/23/2020, in the PS /

00452/2019, where the affected party claims the processing of their data in contracting

of telephone lines without any reason that legitimizes their treatment (article 6.1 of the

GDPR), stating: "The defendant has not provided any document or evidence

any evidence that the entity, in such a situation, would have deployed the diligence

minimum requirement required to verify that indeed your interlocutor was the one who affirmed

I'm going to show off."

And that subsequently the National Court, in a Judgment of 05/05/2021, Rec.

437/2020 established that: "Regarding the face-to-face contracting of the XXXXX-

XXXX It should be reiterated that although a contract is provided, the complainant has not recognized

certifying as his the signature attached thereto, stating the Y that lacks coincidence-

with the one that appears in your DNI, considering the Chamber that the required diligence obligates

was to contrast through the pertinent documentation, the identity of the person facilitating

data, by showing the original identification document and attaching

a copy of the same to the declaration of intent that you want to enforce, as

has been reiterating in similar cases"; stating in the following paragraph:

Therefore, in view of the circumstances set forth, it cannot be appreciated that the
recurring operator to perform due diligence to verify the identity of
the person who associated the controversial telephone lines in their records, therefore
that the subjective element of guilt concurs. On the other hand, regarding the fact
I am aware that we are dealing with a third party fraud, as we said in the SAN of
October 3, 2013 (Rec. 54/2012) -: "Precisely for this reason, it is necessary to ensure
ensure that the person you hire is who they really say they are, and appropriate
appropriate preventive measures to verify the identity of a person whose
personal data will be processed...".

And, in the same sense, in its Judgment of 03/08/2018, Rec 926/2016: “Considering
For this reason, this Chamber, as the Administration understands, that the minimum diligence
required, required TME to verify, through the pertinent documentation
the identity of the person providing the data, by showing the original document
identification document and attaching a copy of it to the declaration of will
that he wants to assert."

The AEPD itself has also ruled, likewise, in its resolution,
06/23/2020, in PS/00452/2019, where the affected party claims the treatment of their data.
in the contracting of telephone lines without any cause that legitimizes their treatment.
(Article 6.1 of the GDPR): "The defendant has not provided a document or element
any evidence that shows that the entity, in such a situation, would have displayed
the minimum diligence required to verify that the interlocutor was indeed the
which he claimed to hold.

However, the aforementioned cases do not bear any similarity with

which we are examining, no matter how much the defendant is interested in proposing it, since it

it deals with fraudulent contracts, due to infringement of the principle of legitimation (article

6.1 of the GDPR) in the first case and the principle of consent (article 6.1 of the

LOPD) in the second and that the defendant should be well aware of the position in the procedure.

The sanctioning party was sanctioned by the AEPD and was a recurring party in the dispute

which gave rise to the first of the sentences, dismissing the appeal filed and

sanctioned with 80,000 euros.

Therefore, the treatment of the image of the DNI at the time of delivery of a

product contracted at a distance not only is it not considered lawful but it is considered

inappropriate not relevant or limited to what is necessary in relation to the purposes for which

that are processed, since it must not be forgotten that the DNI contains data that exceeds and

It has nothing to do with the purpose pursued.

The AEPD in the current case not only is not in contradiction with the resolutions

dictated, but it is consistent and consistent with the interpretation that has been making

the National Court itself in its sentences.

That is why the allegation of the defendant reiterating that the AEPD sanctioned her

Naba for his lack of diligence in not keeping proof of identity verification

of the interested party and in the opening of the current procedure in which he is blamed for

quite the contrary, keeping proof of identity verification of the interested party is not

certain nor can it be accepted as it does not deal with contradictory administrative resolutions.

conflicts between themselves or affect legal certainty, nor generate uncertainty and defenselessness.

Therefore, it is considered that there is a violation of the principle of minimization of

the data being the defendant responsible for the violation of article 5.1.c) of the

GDPR, infringement typified in article 83.5.a).

4. Finally, the defendant invoked the violation of the principle of proportionality
purpose by requesting a reduction in the amount of the penalty by reducing it.

In this regard, it should be noted that taking into account that it is a
offense classified as very serious and that in accordance with article 83 of the
RGPD can be sanctioned, "with administrative fines of €20,000,000 maximum".
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 value". an important reduction of the same is already applied, in addition to
take into account the circumstances and evaluation criteria concurrent in it.

The STS, Chamber 3, of December 16, 2003 (Rec. 4996/98) already indicated that the main
principle of proportionality of the sanctions requires that "the discretion granted
to the Administration for the application of the sanction is developed weighing in all
case the concurrent circumstances, in order to achieve due proportionality
between the facts charged and the responsibility demanded". Principle of proportionality
that it has not been violated, considering the sanction proposed to the entity
based on the proven facts and once the circumstances and criteria that
concur.

For the rest, the specific circumstances that have been taken into account for the
graduation of the amount of the sanction are detailed in Fundament VII of this resolution.
lution.

V

The defendant has alleged his disagreement with the content of the fundamentals
expressed in the Proposal for the procedure ratifying what has already been stated in this

previous crits.

It alleges that it is intended to penalize for displaying an excessive level of diligence

in the identification of its clients by requiring a copy of the DNI, the only document that

in accordance with Organic Law 4/2015, of March 30, Protection of Security

Citizenship that allows to prove the identity and personal data of its owner.

It is true that article 8.1 of the LOPSC establishes that the DNI "is the only document

document with sufficient value on its own for the accreditation, for all purposes, of the

identity and personal data of its owner" and that verification by the re-

claimed the identity of the interested party at the time of delivery of the product to your

domicile is considered lawful both to execute the object of the contract and can be

the delivery of the contracted product and to prevent the commission of fraud. However,

what is in doubt is that the method, protocol, procedure or system carried out

carried out for this is not appropriate, photographing the front and back of the DNI at the same time

time of delivery, for being excessively inappropriate and intrusive in the privacy of the

people, unless it is due to other reasons, such as hiring

tion had not been exercised with reasonable diligence and the

corresponding documents, what need does the defendant have to photograph said

document if it is already in your possession?

It has also alleged that the treatment of the images of the DNI of the interested party

It is not only considered necessary to prove that the product has been delivered to the

person who appears as contracting party, but this criterion has been collected by the

Agency not only in specific resolutions and is also described by the Agency in the

'Officio Inspection Plan on Distance Contracting in Telecom Operators

Communications and Energy Marketers of the AEPD', where the same identifi-

enforces compliance with regulations in the sector and proposes improvements to make effective
that duty of care.

In relation to the Ex officio Inspection Plan on Distance Contracting
in Telecommunications Operators and Energy Marketers of the AEPD',
specifically established in the section 'Accreditation of the identity of the Contractor
te' that prior to the contracting and therefore in a matter that is not similar
jable to what is the object of this procedure as already indicated, figure
that "In the stores of some telephone operators the terminal can be delivered
mobile phone purchased from customers who have contracted by telephone or telematics
cos, in which case the presentation of an official identity document is requested
(DNI, NIE, passport) and a bank document proving that the account on the
that charges are going to be made is owned by the contracting party.

Deliveries are also made using the Post Office service that checks
the client's ID using a scanning system to collect the copy.

Telephone contracts are usually recorded and in cases of portability
ity, a third party performs the verification by third parties".

It is true that the treatment of the images of the DNI in contracting at dis-
tance of a product such as a mobile terminal is not only being considered
considered lawful by the Agency itself, but it is considered that said treatment is co-
Respond with the required diligence.

Therefore, said treatment is necessary so that the defendant can accredit
verify the contracting carried out and that it has been carried out with the due diligence
supporting documentation of the same.

However, in the present case we are not dealing with a case of treatment

unlawful lying; the question to be clarified as to whether the data collected at the time of

the delivery of the mobile terminal have been excessive or not for the purpose pursued,

In the aforementioned Plan it was already indicated (page 8), in relation to the hiring of

distance in the Alerts section that: “Some companies in the sector have identified different

different circumstances that may be susceptible to fraud in contracting (high

concentration of orders in certain areas, same IP addresses...) and have im-

procedures have been established that allow warning of these anomalies and determine the pro-

probability of fraud, in which case, contracts by specialists are usually verified.

lists and additional documentation may be required from the client.

And on page 19, in relation to the identity of the contracting party that:

"Telematic contracts require contract signing and copy of documentation

identification (DNI and bank generally) although it has been detected that it is not always do-

Documentation is recorded in the companies.

• A growing concern has been detected by all companies

to guarantee the identity of the contracting party and for this reason they are studying and implementing

different solutions in order to avoid identity theft as much as possible.

including facial recognition and the electronic handwritten signature.

In this sense, he recommended a series of measures:

- Maximize the guarantees of identification of the contracting party prior to the

execution of the contract,

- The use in systems with additional guarantees of the style of what is defined

in the PSD2 regulations,

-Biometric data.

Well, none of these recommendations included or referred to

to the system or procedure implemented by the claimant for the delivery of products

hired, consisting of photographing the ID using the apps that the delivery man has

installed in your mobile terminal.

However, the Agency itself has considered that this is a question

complex, having to attend to the specific case, to the techniques used in the treatment

ment, interference in the right to data protection, and must, as long as

as long as the European Committee for Data Protection does not pronounce on it or

courts, adopt in case of doubt, the interpretation that is most

favorable for the protection of the rights of those affected.

On the other hand, if the contracting carried out by the defendant of which

has provided a copy of the document signed by the contracting party was correctly identifying

(copy of the DNI and bank document where the account number appears), com-

proving that the identity of the addressee and the contracting party coincide should be done without

need to request again the copy of the DNI (photograph of its front and back)

SW).

SAW

The infringement attributed to the defendant is typified in the

Article 83.5 a) of the GDPR, which considers that the infringement of "the basic principles

for treatment, including the conditions for consent under art.

Articles 5, 6, 7 and 9" is punishable, in accordance with section 5 of the aforementioned article.

Article 83 of the aforementioned Regulation, "with administrative fines of €20,000,000 as

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

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

I know for the largest amount."

The LOPDGDD in its article 71, Violations, states that: "They constitute infringements

tions the acts and conduct referred to in sections 4, 5 and 6 of article 83

of Regulation (EU) 2016/679, as well as those that are contrary to this law

organic".

And in its article 72, it considers for the purposes of prescription, which are: "Infractions

considered very serious:

1. Based on what is established in article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

suppose a substantial violation of the articles mentioned therein and, in part

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.

(…)

In order to establish the administrative fine that should be imposed, they must observe

VII

See the provisions contained in articles 83.1 and 83.2 of the GDPR, which state:

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

pursuant to this article for breaches of this Regulation.

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

constrained and dissuasive.

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

of each individual case, as an addition to or substitute for the measures contemplated

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

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

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

nature, scope or purpose of the processing operation in question

as well as the number of interested parties affected and the level of damages.

cios who have suffered;

b) intentionality or negligence in the infraction;

c) any measure taken by the controller or processor

to alleviate the damages and losses suffered by the interested parties;

d) the degree of responsibility of the data controller or processor

to, taking into account the technical or organizational measures that have been applied

under articles 25 and 32;

e) any prior infringement committed by the controller or processor

I lie;

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

gave to the breach and mitigate the potential adverse effects of the breach;

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

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

particularly if the person in charge or the person in charge notified the infringement and, in such a case,

what extent;

i) when the measures indicated in article 58, paragraph 2, have been ordered

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

relation to the same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or to mechanisms

of certification approved in accordance with article 42, and

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

case, such as the financial benefits obtained or the losses avoided, direct

or indirectly, through the infringement".

In relation to letter k) of article 83.2 of the GDPR, the LOPDGDD, in its article

Article 76, "Sanctions and corrective measures", establishes that:

"2. In accordance with the provisions of article 83.2.k) of the Regulation (EU)

2016/679 may also be taken into account:

a) The continuing nature of the offence.

b) Linking the activity of the offender with the performance of processing

of personal data.

c) The benefits obtained as a consequence of the commission of the infraction.

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

commission of the offence.

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

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

f) The affectation of the rights of minors.

g) Have, when it is not mandatory, a data protection delegate.

cough.

h) Submission by the person in charge or person in charge, voluntarily

party, to alternative dispute resolution mechanisms, in those su-

positions in which there are controversies between those and any interested party."

In accordance with the precepts transcribed, for the purpose of setting the amount of the sanction

tion of a fine to be imposed in the present case for the offense typified in article

83.5 of the GDPR for which the defendant is held responsible, in an initial assessment,

The following factors are estimated to be concurrent:

As aggravating circumstances:

- The nature, seriousness and duration of the infringement: the facts considered

proven seriously affect a basic principle relating to data processing

of a personal nature, such as data minimization; management is questioned

developed by the claimed result of the procedure called Identservice, a

modality of delivery of products implemented for the treatment of data and its

adaptation to the RGPD, being considered inadequate from the moment of collection

of the copy of the DNI both on the front and on the back at the time of delivery

of the package to its recipients. The scope or purpose of the processing operations

since a procedure such as the one implemented and the importance of the entity

ity is not established to operate in a reduced or local scope (article 83.2, a) of the

GDPR).

The number of people potentially affected because, even if it is a

sole claimant, it seems evident that a considerable number may have been affected.

of the entity's customers since in accordance with the loan contract

tion of services held was implemented in January 2019; we must not forget either

that on 06/18/2020 another claim for identical facts was entered in the AEPD

chos (article 83.2, a) of the GDPR).

In this same sense, the conditions of the deliveries of the products that

makes the claim to its clients are detailed on its official website,

through the following link: https://ayuda.orange.es/particulares/movil/mi-movil/mi-

order/1101-where-do-I-pick-up-my-order-and-what-documentation-do I need?

utm_source=orange&utm_medium=SMS&utm_term=smsAltaPedido

- The activity of the allegedly infringing entity is linked to the tra-

Treatment of data of both clients and third parties. In the activity of the re-

clamada is essential to process the personal data of its clients

Therefore, given the volume of business of the same, the importance of the conduct

object of this claim is undeniable (article 76.2.b) of the LOPDGDD in

relation to article 83.2.k).

- The intent or negligence in the infringement since the defendant was

fully aware of the procedure implemented for the delivery of products to

their final recipients. Also connected to the degree of diligence that the respondent

saber of the treatment is obliged to deploy in compliance with the obligations

imposed by the data protection regulations, the SAN of

10/17/2007. Although it was issued before the RGPD entered into force, its pronouncement is

perfectly extrapolated to the assumption that we analyse. The sentence, after

refer to the fact that the entities in which the development of their activity entails a continuous

processing of customer data and third parties must observe an adequate level of diligence

gency, specified that “(...). the Supreme Court has been understanding that there is imprudence

responsibility whenever a legal duty of care is neglected, that is, when the in-

fractor does not behave with the required diligence. And in the assessment of the degree of diligence
The professionalism or otherwise of the subject must be especially considered, and it is not possible to
doubt that, in the case now examined, when the appellant's activity is
constant and abundant handling of personal data must be insisted on the ri-
gor and the exquisite care to adjust to the legal precautions in this regard" (article
83.2, b) of the GDPR).
- The continuous nature of the infringement, since it must not be forgotten that the procedure
performance in accordance with the contract for the provision of services concluded already carries
long implanted. The infringing conduct participates in the nature of
the so-called permanent infractions, in which the consummation is projected in
the time beyond the initial event and extends, violating the protection regulations
data, during the entire period of time in which the data is processed.
I lie. In this sense, the judgments of the National Court of
09/16/2008 (rec.488/2006) and the Supreme Court of 04/17/2002 (rec. 466/2000) (ar-
article 76.2.a) of the LOPDGDD in relation to article 83.2.k).
In the present case, having valued the criteria that concur in it for the
graduation of the sanction, a sanction of 100,000 euros is imposed for violation
of article 5.1.f) of the GDPR, for which the defendant must respond.
Therefore, in accordance with the applicable legislation and assessed the criteria of
graduation of sanctions whose existence has been accredited,
The Director of the Spanish Data Protection Agency RESOLVES:
FIRST: IMPOSE ORANGE ESPAGNE, S.A.U., with NIF A82009812, for a
infringement of Article 5.1.c) of the GDPR, typified in Article 83.5 of the GDPR, a
fine of €100,000 (one hundred thousand euros).
SECOND: NOTIFY this resolution to ORANGE ESPAGNE, S.A.U.
THIRD: Warn the penalized person that they must make the imposed sanction effective

Once this resolution is enforceable, in accordance with the provisions of Article

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations (hereinafter LPACAP), within the payment term

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, by means of its income, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted number ES00 0000 0000 0000 0000 0000, open in the name of the Agency

Spanish Data Protection Agency at the bank CAIXABANK, S.A.. In the event

Otherwise, it will proceed to its collection in the executive period.

Once the notification has been received and once executed, if the execution date is

between the 1st and 15th of each month, both inclusive, the deadline for making the

voluntary payment will be until the 20th day of the following or immediately following business month, and if

is between the 16th and the last day of each month, both inclusive, the term of the

Payment will be until the 5th of the second following or immediate business month.

Against this resolution, which puts an end to the administrative process in accordance with art.

48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the

LPACAP, interested parties may optionally file an appeal for reversal

before the Director of the Spanish Data Protection Agency within a period of one

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

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

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

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

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

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

referred Law.

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

LPACAP, the firm resolution may be temporarily suspended in administrative proceedings

If the interested party expresses his intention to file a contentious appeal-

administrative. If this is the case, the interested party must formally communicate this

made by writing to the Spanish Agency for Data Protection,

presenting it to

the agency

[https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other

records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also

must transfer to the Agency the documentation that proves the effective filing

of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within a period of two months from the

day following the notification of this resolution, would terminate the

injunction suspension

Electronic record of

through the

Mar Spain Marti

Director of the Spanish Data Protection Agency