 File No.: PS/00078/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

BACKGROUND

FIRST: Dated 01/08/2019, through the “Market Information System Interior” (hereinafter IMI), regulated by Regulation (EU) No. 1024/2012, of the European Parliament and of the Council, of October 25, 2012 (IMI Regulation), whose objective is to promote cross-border administrative cooperation, mutual assistance between the Member States and the exchange of information, was received in this Spanish Agency for Data Protection (AEPD) a claim made by A.A.A. (hereinafter the claimant), a Dutch citizen, before the authority of Netherlands data protection (Autoriteit Persoonsgegevens -AP). The transfer of This claim to the AEPD is made in accordance with the provisions of article 56 of Regulation (EU) 2016/679, of the European Parliament and of the Council, of 04/27/2016, regarding the Protection of Natural Persons with regard to the Processing of Personal Data and the Free Circulation of these Data (as successive General Data Protection Regulation or RGPD), taking into account its cross-border nature and that this Agency is competent to act as main controlling authority.

The aforementioned claim is made against the entity MARINS PLAYA, S.A. (in hereinafter MARINS PLAYA or claimed entity), with registered office in Spain, for the following reasons:

The claimant indicates that in the hotel registration process they asked for his passport, which was digitally scanned, despite his opposition. The client objects to

said document was completely scanned, alleging that not all the data

included in it are necessary, to which the hotel employee replied that

said scanning was carried out following instructions from the police. Secondly,

He claims to have seen the hotel employees with the passport photo on their tablets.

In relation to the issue raised by the complainant, the referring authority

He asked if the Spanish law really obliges to scan the passport completely or

only some information is necessary to complete the registration process.

According to the information included in the IMI System, in accordance with the

established in article 60 of the RGPD, have declared themselves interested in this

procedure the supervisory authority that has communicated the case (the Netherlands).

SECOND: In view of the exposed facts, the Subdirectorate General of Inspection

of Data proceeded to carry out actions for its clarification, under the protection of the

investigative powers granted to the control authorities in article 57.1 of the

GDPR. Within the framework of these actions, a request was addressed to the entity

claimed, which reported the following:

1. Upon check-in, the client's passport is scanned in order to

to pass the image to text for the incorporation of the fields corresponding to the

hotel management program

2. Only the page on which the ID is found is scanned.

client: the identification data of the traveler, including the number,

type and date of issue of the identity document presented, name and

surnames, sex, date and country of birth, as well as photography.

3. There are no specific instructions from the Security Forces and Bodies of the

State on the copying of the aforementioned document, except those related to the telematic delivery

of the information.

4. The information is also used, accounting, to generate the

corresponding invoices; can only be accessed by administrative staff

accounting.

5. When the client registers, he is provided with a magnetic card that

allows, in addition to access to the room, the payment of consumption charged to your

account to be paid at the end of your stay; at the time of consumption, the

customer provides this card to the employee, who, by swiping it to make the charge, can

check passport photo. This is to verify the identity of the

customer, in order to prevent fraudulent use of the card by third parties and prevent

cause serious economic damage to the customer. You can only see the photo

employee who collects, on the POS tablet.

6. The applicable regulations for the identification of clients in the registration process

or registration in the hotel is the Organic Law 4/2015, of March 30, on the protection of

citizen security and Order INT/1922/2003 of July 3.

THIRD: After reviewing the answers obtained during the previous phase of

investigation, outlined in the previous Fact, this Agency considered that the

processing of personal data object of the claim is legitimized by

article 6.1.c) of the RGPD and is proportionate and necessary in accordance with the

established in article 24 of the aforementioned Organic Law 4/2015, which provides in its

First section: “The natural or legal persons who carry out relevant activities

for citizen security, such as lodging… will be subject to the

obligations of documentary registration and information in the terms established by the

applicable provisions". And that is detailed in the aforementioned Order (Order

INT/1922/2003 of July 3).

On the other hand, it was taken into account that the facts denounced were not verified.

referred to the scanning of all the pages of the passport.

Second, it was concluded that the processing of personal data consisting of

the use of the photograph obtained from the passport in order to verify identity

of the client in the consumptions that he makes, when making charges in the account of a

room, and prevent fraudulent use of the hotel card by third parties

other than the user of the service, is legitimized in article 6.1.f) of the RGPD, since

there is a legitimate interest on the part of the hotel in charging the true user of the service

and for the customer, since the cards are prevented from being used fraudulently and

charge the account of a client the consumption made by others.

Consequently, having clarified the doubts raised, it was considered that there were no

indications of infraction, for which, on 09/28/2020, a Project of

File resolution of the claim (Draft decision).

FOURTH: On 11/10/2020, the Draft Decision was incorporated into the IMI System

so that the interested authorities could express themselves in this regard.

At the end of the established period, the

Dutch data protection authority (Autoriteit Persoonsgegevens - AP).

Regarding the facts, said supervisory authority warns that the claimant

stated that the hotel staff had on their device the complete copy of

your passport (first page), including your photo, and that this differs slightly from what indicated in the Draft Decision, although it does not change the evaluation carried out on the same.

The AP admits that the processing of personal data collected in the passport (number, type and date of issue of the identity document presented, name and surnames, sex and the date and country of birth, as well as the photograph) is necessary for compliance with national legislation and, therefore, lawful in accordance with the article 6.1.c) of the RGPD, but questions the processing of said personal data in under the provisions of article 6.1.f) of the same RGPD, due to the existence of a legitimate interest of the responsible hotel in avoiding the fraudulent use of the card that provides to customers, which is used to make consumption in the facilities and also as a room key; and also of the client, since it prevents the cards are used fraudulently and you are charged for consumption made by others.

Regarding this processing of personal data based on legitimate interest, the AP to the requirement of necessity, which requires assessing proportionality and subsidiarity of the treatment, verifying that such interests cannot be reasonably achieved effectively by other means less restrictive of the rights and freedoms of the interested parties, in particular the rights to respect for life privacy and the protection of personal data guaranteed by articles 7 and 8 of the letter. And it adds that the Court of Justice of the European Union declared, in addition, that the requirement relating to the need for treatment should be examined, together, with the principle of "minimization of data" enshrined in article 5.1.c) of the GDPR.

In this case, the AP notes, there are other, less intrusive ways to check if the magnetic card holder is the legitimate card holder at the time of payment and, thus, prevent said cards from being used fraudulently.

As an example of these less intrusive actions, it indicates the possibility that the

employee of the hotel, when some consumption occurs, consult some data of

control the customer, such as last name or room number, to verify if it matches

with the legitimate cardholder; or require the signing of a receipt for consumption, which

it also acts as a barrier for third parties. In case of loss of the card, it

can be blocked to prevent fraudulent use

The combination of the above scenarios requires a minimum amount of

additional data processing, is less intrusive, and conforms to the principle of

data minimization. Even so, they make it possible to achieve the interests pursued with

common practices in most hotels.

Against this, the additional efficiency provided by the use of the personal data of the

passport to prevent fraud does not overcome the invasion of data protection.

You understand that this data may be used for identity fraud in the event of a

data breach or abuse by hotel employees who have access to

the same, so that their use is not considered proportionate to avoid possible

fraud in the payment of hotel services.

According to the AP, the treatment of all this data is contrary to the principle of

data minimization in accordance with article 5.1.c. of the RGPD, since the

treatment of only a name and room number is sufficient to minimize

fraud effectively. Also, some of the data categories above

mentioned may be considered special categories of personal data of

in accordance with article 9 of the RGPD, without any application

of the exceptions of article 9.2 of the RGPD.

In short, the AP does not share that the use of passport data is allowed

under article 6.1.f of the RGPD in the indicated circumstances. This could

lead to the use of passport data by many hotels and service providers

similar, to a broader use that could give rise to identity fraud in

cases of data breaches or abuse by hotel employees who

have access to them, so that, given the risk to freedoms and

expressed rights, does not consider its use proportionate to avoid possible fraud

in the payment of hotel services.

If a hotel wants to process passport data for identity verification purposes

of clients during their stay, adds the AP, the hotel must invoke another reason for the

article 6 of the RGPD, such as consent, or return to the most common practice, such as

has been described above.

FIFTH

: Dated 05/11/2021, by the General Subdirectorate for Data Inspection

You can access the information available on the MARINS PLAYA entity in “Axesor”.

(...). The aforementioned entity is registered in the economic activity code

corresponding to "Hotels and similar accommodation".

(...).

SIXTH: On 06/03/2021, in accordance with the provisions of article 64 of

the LOPDGDD, sections 2 (third paragraph) and 3, draft agreement to start

sanctioning procedure, motivated by the claim received through the

IMI system that is outlined in the First Precedent. This project takes

consideration the objections outlined in the Fourth Precedent (draft of

revised decision).

Following the procedure established in article 60 of the RGPD, dated

06/25/2021, the aforementioned project to open the sanctioning procedure was

transmitted via the IMI System to the supervisory authority concerned, making it

know that if no objections are raised within two weeks

from the consultation, the mandatory agreement to open the procedure would be adopted

sanctioning

The control authority concerned did not raise any objection to the draft agreement

of opening of sanctioning procedure adopted by the AEPD, understanding, by

So much so that there is agreement on it.

In accordance with the provisions of article 64 of the LOPDGDD, the draft

agreement to initiate the aforementioned sanctioning procedure was notified to the entity

claimed.

SEVENTH: On 06/15/2021, this Agency received a brief presented by the

claimed entity in which it requests the file of the actions in accordance with the

following considerations:

1. Describes the procedure followed in the processing of personal data of

a client from his arrival at the hotel, indicating that the documentation is requested

proof of the identity of all people over 16 years of age who are staying

at your facility, which undergoes a scanning process for the process of

registry, which completes the data collection form without saving in the systems

computers the image of the document.

It is an optical character recognition known by the acronym OCR

(“Optical Character Recognition”), which enables the digitization of texts (the process

automatically identifies the characters of a certain alphabet and stores them

in data form). According to the claim, this process only applies to the page of the

document in which the traveler is identified, collecting personal data relating to

the number, type and date of issue of the document in question (DNI, passport,

driving license, residence permit or identity card), name, surname,

gender, date and country of birth, as well as the photograph. Next, collect the

traveler's signature in digital format, through a Tablet, in which information is given about the

personal data protection regulations; and a card is provided

access to the rooms, also used for the use of hotel services.

The data is processed by the administration and services staff (bar and

dining room) for the payment of consumption. In addition, they are referred to the Forces and

State Security Bodies, in compliance with security regulations

citizen.

2. He denies that the hotel staff had on his device the complete copy of

the first page of the claimant's passport, since the only data that appears

in the devices used by bar and dining room staff with access to POS are

the room number, date of departure, name and surname of the traveler, photograph and

accommodation regime, necessary to carry out the maintenance, development and

negotiation control, legitimizer of the treatment. In this regard, it highlights that, of the

data available on those devices, only the name, surnames and photograph

are taken from check-in).

3. Taking into account the data used to control consumption and
avoid the fraudulent use of the facilities, does not understand the claim that is
questions the legitimate interest, especially when the Agency itself admits the
treatment of personal data collected in the passport for the fulfillment of
national legislation, considering it lawful in accordance with article 6.1.c) of the
GDPR.

On the least intrusive ways to identify the client referred to in the
opening agreement, points out that verbally requesting the room number or the
surname is insufficient and does not prevent another person from hearing these data and
using them; the same as the signing of a receipt, which the employee could not check.

It adds that for these reasons photography was included in the digital systems of the
bar and dining room staff, as a means of authentication, even when the customer is not
is in possession of the card due to forgetfulness, loss or theft.

Regarding the risks in case of a possible data breach, it warns that it has
implemented the mechanisms established in the RGPD and that the employees have
signed a confidentiality agreement.

4. The claimed party does not treat special categories of personal data in any
moment. On this matter, he states that the client's image is only a
photograph from which biometric templates are not extracted or used to
facial recognition or other specific means. Therefore, in his opinion, the treatment
he makes of obtaining the photograph he takes does not fit the concept of
treatment of special categories of data (Considering 51 and article 4.15 of the
GDPR).

Consequently, the claimed entity concludes that the processing of the data

used to authenticate the identity of the person making an expense does not violate the

provided in article 6.1.f) of the RGPD, as it is necessary for the satisfaction of

legitimate interests pursued by the data controller (avoid damages and

lawsuits for improper charges), as well as the interested party (avoid improper charges).

Provides a photograph in which you can see the detail of the information available in

the devices of the hotel staff on a specific person: in the section

“Reservation data” includes the room number, reservation number, number

of people and date of departure; in the section “Components of the reservation” it is indicated

the name and surname of the person, status, type of VIP and number of visits, in addition

of the client's photograph.

EIGHTH: On 07/19/2021, the Director of the Spanish Protection Agency

of Data agreed to initiate sanctioning proceedings against the entity MARINS PLAYA, with

in accordance with the provisions of articles 63 and 64 of Law 39/2015, of October 1, of the

Common Administrative Procedure of Public Administrations (hereinafter,

LPACAP), for the alleged infringement of article 6 of the RGPD, typified in article

83.5.a) of the same Regulation, and classified as very serious for prescription purposes

in article 72.1.b) of the LOPDGDD; determining that the sanction that could

correspond, considering the evidence existing at the time of opening and

without prejudice to what results from the instruction, it would amount to a total of 30,000 euros

(thirty thousand euros).

In the same agreement to open the procedure, it was noted that the infringement

charged, if confirmed, may lead to the imposition of measures, in accordance with

the provisions of the aforementioned article 58.2 d) of the RGPD.

NINTH: Having been notified of the aforementioned initiation agreement, the respondent submitted a written

dated 07/22/2021, in which it again requests the file of the procedure

sanctioning

In this new letter, he literally reproduces his previous allegations, which include

outlined in the Seventh Antecedent. It only adds that Recital 47 of the

RGPD admits the processing of personal data necessary for the prevention of

fraud based on the legitimate interest of the person in charge and that is considered fraud a

economic deception carried out with the intention of making a profit, and with the

which someone is harmed.

TENTH: On 08/24/2021, the instructor of the procedure agreed to open

a period of practice of evidence, considering reproduced for evidentiary purposes

the claim filed, the documents obtained and generated by the Subdirectorate

General Data Inspection and Inspection Services, and the Report of

Previous Inspection Actions that are part of file E/01088/2019; Y

for submitting the allegations made by MARINS PLAYA and the documentation

that accompanies them.

Likewise, it was agreed to require the entity the entity claimed to provide the

following information and/or documentation:

“a) Copy of the record of all the activities of treatment of personal data of clients

carried out under the responsibility of MARINS PLAYA. This register, to which the

Article 30 of the RGPD, must be provided in its initial version, together with any additions,

modification or exclusion in the content of the same.

b) If you have them, a copy of the assessment(s) of the impact on data protection

related to any type of personal data processing operations of

clients made under the responsibility of MARINS PLAYA that involve a high risk

for the rights and freedoms of natural persons.

The initial version of this/these impact assessment(s) must be provided and, if applicable, the details

of the modifications or updates that may have been made.

Likewise, if there has been a change in the risk represented by the operations of

treatment and if deemed necessary, you must provide the result of the examination that

MARINS PLAYA has been able to carry out to determine if the treatment is in accordance with the

impact assessment related to data protection (article 35.11 of the RGPD).

c) Copy of the documents in which the evaluation carried out on the prevalence or not

of the interests and fundamental rights of customers against the interests of MARINS

PLAYA, in relation to customer personal data processing operations

carried out under the responsibility of MARINS PLAYA with which satisfaction is intended

of legitimate interests pursued by the MARINS PLAYA entity itself or by a third party.

d) Copy of the information on data protection (privacy policy) provided

through any channel to the clients of that entity, in its current version and versions

previous ones in force as of 05/25/2018, where appropriate, with an indication of the period of validity

of each version.

If there were addenda or variations, or other privacy notices or additional information,

regarding the processing of personal data, a copy of all documents is requested

employees to report on the protection of personal data other than the privacy policy

privacy.

e) Detail of the channels and procedures enabled to make known to its clients all the information regarding the protection of personal data (privacy policy or any another document).

f) Information regarding the channels, mechanisms and methodology used by that entity to obtain the acceptance by its clients of the privacy policy or any other document used by that entity to report on data protection personal; as well as for the provision of the consents provided for in such documents, in your case.

g) Screen prints corresponding to all the information that is registered in your information system related to the claimant in the sanctioning file of reference.

h) Details of the computer program used by that entity to collect the data of customers by scanning documents and converting them to text".

In response to this request, this Agency received a letter from the respondent accompanied by the documentation indicated below. In this writing, said entity stated that it could not provide the impressions of the bar and dining room tablets with the claimant information available on these devices because This information is deleted at the time the client checks out, nor the Wi-Fi accesses, where appropriate, which are deleted after twelve months (Law 25/2007).

From the content of the documentation provided, the following should be noted:

1. Registration of customer personal data processing activities.

. Purpose: accounting, fiscal and administrative management;

. Category of interested parties: clients and users;

. Types of data: DNI or NIF, name and surnames, postal or electronic address, telephone, image and manual signature;

. Other types of data: personal characteristics, social circumstances, information commercial, transactions of goods and services;

. Transfers: Security Forces and Bodies.

. Access to equipment: it is accessed through a personalized username and password.

2. Risk analysis on the treatment of personal data of clients.

After analyzing the data structure, regulatory compliance, the organization

and resources, as well as security by design and by default, it is concluded that "there is no

there are risks in the resources used".

3. Information on data protection (privacy policy) provided to

www.aepd.es

C/ Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

through the website of the claimed entity.

a) Provide a copy of the "Registration Sheet", which includes a section on the

establishment and another to the "traveler data" (identity document number,

type of document and date of issue, name, surname, gender, date of

birth, country of nationality, date of entry and traveler's signature). This sheet"

includes an informative legend on the protection of personal data that

details, among other aspects, the identity of the person in charge, the purpose for which

the data will be processed, the non-existence of data communications except for

legal obligation, the rights of the interested party, mode of exercise and possibility of

file a claim with the AEPD.

An update of this "Registration Sheet" (2019) is attached, which contains a

new informative clause. This information is provided on the collection and treatment of

data for the purpose of prevention, investigation, detection or prosecution of

criminal offenses under the Organic Law 4/2015, of March 30, of

Protection of Citizen Security; that the data will be kept for three

years and will be available to the Security Forces and bodies; rights of the

interested parties and how to exercise them and the possibility of claiming before the AEPD.

On the other hand, the claimed entity provides a copy of the data protection policy

available on their website. It is distributed in two parts, which it calls “Policy of

Privacy” and “Second layer clauses” (this last part is divided into

epigraphs: reservation client file, invoices/accounting, newsletter, web users,

employees, etc).

The “Privacy Policy” section refers to the personal data collected from

clients “in order to provide them with the contracted services consisting of the

reservation of accommodation in hotel establishments”.

In the information of "Second layer", epigraph "Client reservation file" it is reported

that the defendant processes the information that customers provide "in order to provide them with

the service and sell the requested products, make the billing of the same and

manage the sending of information and commercial prospecting”.

In this information, nothing is indicated about the use of the client's photograph to

consumption control and avoid fraudulent use of the facilities.

4. Screen printout corresponding to the registered information regarding the

claimant (data during check-in). It is presented with the label “Loading data from

the client file”, and includes fields related to name and surname, number of

document and date of issue, nationality, date of birth, last visits and

Photography. According to this information, the entry into the claimant's hotel took place in

date 08/27/2018.

5. Details of the computer program (***PROGRAMA.1”) used to take

of customer data by scanning documents and converting them to text,

provided by the software developer company:

“Customer data capture procedure by scanning documents.

At the time of entering the hotel, the client is asked for their DNI/PASSPORT to make

scanning that document. In this scan and through an OCR process (of the

company…) the data is captured and integrated into the database as it is necessary

to complete 2 essential documents in the normal operation of the hotel:

1. Fill in the passenger entry part. The collection and processing of these data will be done

in accordance with Regulation (EU) 2016/679, of April 27 (GDPR) and Organic Law 3/2018, of 5

of December (LOPDGDD), for the purpose of prevention, investigation, detection or

prosecution of criminal offenses, and under the Organic Law 4/2015, of 30

March, Protection of Citizen Security, article 25.1.

2. Issuance of billing for expenses incurred at the hotel.

The image with the client's photo is captured and saved to secure the credit process to

customers in the different departments as it makes it easier for the hotel staff to identify the

customer who is using the credit or room card. Likewise, it allows

identify said client by the hotel staff when controlling access to the

establishment".

ELEVENTH: On 11/29/2021, a resolution proposal was formulated in the

following sense:

1. That the Director of the Spanish Data Protection Agency sanction

the entity MARINS PLAYA, for an infringement of Article 6 of the RGPD, typified in the

Article 83.5.a) of the RGPD and classified as very serious for the purposes of prescription in the

article 72.1.b) of the LOPDGDD, with a fine of 30,000 euros (thirty thousand euros).

2. That the Director of the Spanish Agency for Data Protection imposes

the entity MARINS PLAYA, S.A., within the period determined, the adoption of the

necessary measures to adapt their actions to data protection regulations

personal, with the scope expressed in the Legal Basis VI of the aforementioned

resolution proposal.

TWELFTH: Notification of the aforementioned resolution proposal, dated

12/15/2021 a letter is received from the entity claimed in which it reiterates its request for

archive of the procedure, basing its request on the following allegations:

1. The claimant, during the registration process at the hotel establishment, who

took place on 08/27/2018, three months after the entry into force of the RGPD, facilitated

your passport without showing any opposition. At that time he was informed about the

extremes imposed by the RGPD through an informative document written in

Spanish and had at its disposal a "display" with an informative clause regarding the

data processing carried out. Currently, this information is provided in

the most frequent languages among the entity's clients.

2. Recital 47 of the RGPD expressly states that the treatment of

personal data strictly necessary for the prevention of fraud constitutes

also a legitimate interest of the controller, which operates "ex lege"

when the treatment obeys this purpose and the parameters that must be

be taken into account to carry out the weighting, such as whether the interested party is

client or is at the service, the performance of a prior analysis and that the treatments do not

occur in circumstances in which the interested party does not expect that a

further treatment (the data subject's perspective).

In this case, the first aspect is given; the second was the object of analysis when implemented the technological solution for check-in, concluding the need for inform, limit access to the image exclusively to payment operators for consumption and keep the data only during the client's stay; Besides, the identification by image has been favorably valued by customers, as they have avoided erroneous charges, especially when “all-in” stays are offered. included".

3. There are no alternatives that offer the same guarantee minimizing the treatment of the personal information.

Reiterates that the proposals of the Dutch data protection authority about other less intrusive practices, such as consulting the interested party of some data (surname or room number) or the signature of a receipt, are not effective or involve the processing of other data, such as the signature, which are not less demanding of protection.

4. The image of the client is only displayed by the personnel that attends the payments by consumption, who sign a confidentiality document, no other treatment of said image and is eliminated at the end of the client's stay.

5. The arguments upheld by the respondent is the one upheld by the Agency itself when it initially considered that there were no indications of infringement.

With its brief of allegations, MARINS PLAYA provides a copy of the document information to which he refers in his allegations. This document explains the check-in process and treatment of the image of the identification document using a character recognition program. In relation to photography

the following is indicated:

"Likewise, the photo that appears in the passport or DNI that you have provided for check-in

will be registered in the hotel management system of the destination hotel. The purpose is to allow the

hotel staff identify you as a guest and control the charge for consumption

that you make during your stay in your room. This photo will be deleted at the time of

check out.

This treatment is based on our legitimate interest in identifying hosted customers

for security and charge control purposes. For the weighting of this interest with respect to

your rights and freedoms it has been determined that the treatment had a limited impact on your

privacy, because:

- There is a contractual relationship and the treatment is carried out in connection with said relationship;

- This security measure benefits the customers themselves by guaranteeing the correct imputation

of the charges to your room and avoid possible impersonations;

- Access to your image is restricted to hotel staff;

- The term of conservation of your image is limited to the time of your stay".

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited:

PROVEN FACTS

1. The entity MARINS PLAYA is dedicated to the provision of hotel services and

of similar accommodation.

2. For customer registration (check-in), at the time of their arrival at the

hotel, requests identification documentation and submits it to a scanning process

that enables the digitization of texts (the process automatically identifies the

characters of a given alphabet and stores them as data), by

an optical character recognition (OCR) computer program. This process

converts the image into text and incorporates the data into the hotel management program,

filling in the "customer file" or "traveler entry part", with fields

regarding the number, type and date of issue of the identity document presented,

name and surname, sex, date and country of birth. This process applied by

The claimed entity also incorporates the client's photograph into its database.

At this time, the customer is provided with a magnetic card that can be used both

for access to the room and to make use of the hotel services.

3. The data collected from the client by MARINS PLAYA is processed by the staff of

administration and services (bar and dining room); and are sent to the Forces and Bodies

of State Security, in compliance with citizen security regulations.

Service personnel use a device that has embedded information regarding

to clients: in the “Reservation data” section, include the room number,

reservation number, number of people and departure date; in section

"Components of the reservation" indicates the name and surname of the person, regime,

type of VIP and number of visits, in addition to the client's photograph.

The entity MARINS PLAYA has stated that the image with the client's photo is

used to make it easier for hotel staff to identify the client who is doing

use of the credit card or room (at the time of making a consumption, the

customer provides this card to the employee, who, by swiping it to make the charge, can

check the photograph), as well as to control access to the establishment.

4. The Record of Treatment Activities (RAT) provided by MARINS PLAYA

includes the following information on the processing of personal customer data:

. Purpose: accounting, fiscal and administrative management;

. Category of interested parties: clients and users;

. Types of data: DNI or NIF, name and surnames, postal or electronic address,

telephone, image and manual signature;

. Other types of data: personal characteristics, social circumstances, information

commercial, transactions of goods and services;

. Transfers: Security Forces and Bodies.

. Access to equipment: it is accessed through a personalized username and password.

5. MARINS PLAYA has stated during the investigation of the procedure that

after the scanning of the client's identification document, carried out during the

registration process, the traveler's signature is collected in digital format, through a Tablet,

which informs about the personal data protection regulations.

MARINS PLAYA has provided the actions with a copy of the "Registration Sheet", which

includes a section relating to the establishment and another to "traveler data" (number of

identity document, type of document and date of issue, name, surname,

gender, date of birth, country of nationality, date of entry and traveler's signature).

This "Sheet" includes an informative legend on data protection

that details, among other aspects, the identity of the person in charge, the purpose

for which the data will be processed, the non-existence of data communications except

by legal obligation, the rights of the interested party, mode of exercise and possibility of

file a claim with the AEPD.

There is also an update of this "Registration Sheet" (2019) that contains a

new informative clause. This information is provided on the collection and treatment of

data for the purpose of prevention, investigation, detection or prosecution of

criminal offenses under the Organic Law 4/2015, of March 30, of

Protection of Citizen Security; that the data will be kept for three

years and will be available to the Security Forces and bodies; rights of the

interested parties and how to exercise them and the possibility of claiming before the AEPD.

6. MARINS PLAYA has contributed to the actions the detail on the information in

matter of data protection (privacy policy) that it facilitates through its website.

In this information, nothing is indicated about the use of the client's photograph to

consumption control and avoid fraudulent use of the facilities.

7. The personal data of the claimant are registered in the System of

Information about MARINS BEACH. It is presented with the label “Loading data from the file

of the client”, and includes fields related to name and surname, document number and

date of issue, nationality, date of birth, last visits and photograph.

According to this information, the entry into the claimant's hotel took place on the date

08/27/2018.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each Authority of

Control and, as established in articles 47, 64.2 and 68.1 of the LOPDGDD, the

Director of the Spanish Data Protection Agency is competent to initiate

this procedure.

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

Spanish Agency for Data Protection will be governed by the provisions of the RGPD, in

this organic law, by the regulatory provisions issued in its

development and, in so far as they are not contradicted, on a subsidiary basis, by the rules

general administrative procedures.

Sections 1) and 2), of article 58 of the RGPD, list, respectively, the

investigative and corrective powers that the supervisory authority may provide to the

effect, mentioning in point 1.d) that of: “notify the person in charge or in charge of the

treatment of alleged violations of this Regulation”; and in 2.i) that of:

“impose an administrative fine under article 83, in addition to or instead of the

measures mentioned in this section, according to the circumstances of each

case".

The case examined is motivated by a cross-border claim

filed with the Dutch data protection authority (Autoreit

Persoonsgegevens -AP), against MARINS PLAYA, which is based in Spain. Bliss

Headquarters is the principal place of business of said entity, within the meaning of the definition

of article 4.16 of the RGPD. Thus, in accordance with the provisions of article 56.1 of the RGPD,

the AEPD is competent to act as the main control authority.

The following "definitions" established in article 4 of the

GDPR:

“16) main establishment:

a) with regard to a data controller with establishments in more than one

Member State, the place of its central administration in the Union, unless the decisions

about the purposes and means of the treatment are taken in another establishment of the person in charge

in the Union and the latter establishment has the power to enforce such decisions, in

in which case the establishment that has adopted such decisions will be considered

main establishment.

“21) supervisory authority: the independent public authority established by a State

member in accordance with the provisions of article 51”.

“22) interested control authority: the control authority that is affected by the treatment of

personal data because:

a.- The controller or processor is established in the territory of the State

member of that control authority;

b.- Interested parties residing in the Member State of that control authority are

substantially affected or likely to be substantially affected by the

treatment, or

c.- A claim has been filed with that control authority”.

“23) cross-border processing:

a) the processing of personal data carried out in the context of the activities of

establishments in more than one Member State of a person in charge or a person in charge of the

processing in the Union, if the controller or processor is established in more than one

Member state,

or b) the processing of personal data carried out in the context of the activities of a single

establishment of a controller or a processor in the Union, but which affects

substantially or is likely to substantially affect data subjects in more than one State

member".

According to the information included in the IMI System, in accordance with the

established in article 60 of the RGPD, in this procedure acts as

of "interested control authorities" the personal data protection authority

of the Netherlands (Autoriteit Persoonsgegevens -AP).

II

Article 56.1 of the RGPD, regarding the "Competence of the supervisory authority main", states the following:

"1. Without prejudice to the provisions of article 55, the control authority of the establishment main or sole establishment of the controller or processor will be competent to act as lead supervisory authority for cross-border processing carried out by said person in charge or person in charge in accordance with the established procedure in article 60".

Said article 60 regulates the "Cooperation between the main control authority and the other interested control authorities":

"1. The main control authority will cooperate with the other control authorities stakeholders in accordance with this article, striving to reach a consensus. The main control authority and the control authorities concerned will exchange all relevant information.

2. The main control authority may at any time request other authorities of Control interested parties that provide mutual assistance in accordance with article 61, and may carry out conduct joint operations under article 62, in particular to carry out investigations or supervise the application of a measure related to a person in charge or a processor established in another Member State.

3. The main control authority shall promptly notify the other control authorities relevant information in this regard. It will transmit without delay a project of

decision to the other control authorities concerned to obtain their opinion on the matter

and will take due account of their views.

4. In the event that any of the interested control authorities raises an objection

relevant and reasoned information on the draft decision within four weeks of

consultation pursuant to paragraph 3 of this article, the lead supervisory authority

will submit the matter, in case it does not follow what is indicated in the pertinent and motivated objection or

considers that said objection is not pertinent or is not motivated, to the coherence mechanism

referred to in article 63.

5. In the event that the main supervisory authority plans to follow what is indicated in the objection

pertinent and reasoned received, it will submit to the opinion of the other control authorities

stakeholders a revised draft decision. This revised draft decision is

will submit to the procedure indicated in section 4 within a period of two weeks.

6. In the event that no other interested supervisory authority has objected to the

draft decision transmitted by the main supervisory authority within the period indicated in the

paragraphs 4 and 5, it will be considered that the main supervisory authority and the authorities of

Stakeholders are in agreement with said draft decision and will be bound by

East.

7. The main control authority will adopt and notify the decision to the main establishment

or to the sole establishment of the person in charge or the person in charge of the treatment, as appropriate, and

shall inform the interested control authorities and the Committee of the decision, including a

summary of relevant facts and motivation. The supervisory authority before which the

submitted a claim will inform the claimant of the decision.

(…)

12. The main supervisory authority and the other interested supervisory authorities

will reciprocally provide the information required within the framework of this article by

electronic means, using a standardized form.

On the issues regulated in these precepts, what is stated in

Recitals 124, 125, 126 and 130 of the RGPD, in particular the following:

(124) "… Said authority (the main authority) must cooperate with the other authorities

interested…".

(125) "As the lead authority, the supervisory authority must closely involve

and coordinate the control authorities interested in the decision-making process".

(126) "The decision must be agreed jointly by the main control authority and the

interested control authorities…".

(130) "When the supervisory authority before which the claim has been filed is not the

lead supervisory authority, the latter must cooperate closely with the former with

in accordance with the provisions on cooperation and coherence established in this

Regulation. In such cases, the lead supervisory authority, by taking measures designed

to produce legal effects, including the imposition of administrative fines, must take into account

account to the greatest extent possible the opinion of the supervisory authority before which the

filed the claim and which must remain competent to perform any

investigation on the territory of its own Member State in liaison with the supervisory authority

competent".

In accordance with the provisions of article 4.24 of the RGPD, it is understood by "objection

relevant and motivated" the following:

"The objection to a proposal for a decision on the existence or not of an infringement of this

Regulation, or on the conformity with the present Regulation of actions foreseen in

relationship with the person in charge or the person in charge of the treatment, which clearly demonstrates the significance of the risks posed by the draft decision to the rights and freedoms of the interested parties and, where appropriate, for the free circulation of personal data within the Union".

In accordance with the provisions of the previous rules, in this case, referred to a claim filed with the supervisory authority of a State member (Netherlands), in relation to processing in the context of activities of an establishment of a person in charge that affect or are likely to affect substantially to data subjects in more than one Member State (data processing cross-border), the main control authority, in this case the Spanish Agency of Data Protection, is obliged to cooperate with the other authorities interested.

The Spanish Agency for Data Protection, in application of the powers that conferred by the RGPD, is competent to adopt the decisions designed to produce legal effects, whether it be the imposition of measures that guarantee the compliance with regulations or the imposition of administrative fines. Nevertheless, is obliged to closely involve and coordinate the control authorities stakeholders in the decision-making process and take their opinion into account in the greater extent. It is also established that the binding decision to be adopted jointly agreed.

Article 60 of the GDPR regulates this cooperation between the main control authority and the other interested control authorities. Section 3 of this article expressly establishes that the main supervisory authority will transmit to the other control authorities concerned, without delay, a draft decision to obtain its opinion on the matter and will take due account of its views, following the procedure provided for in sections 4 and following. The

interested control authorities have a period of four weeks to

raise reasoned objections to the draft decision, on the understanding that

There is agreement on said project if no authority presents objections in the

indicated period, in which case all of them are bound by the repeated project.

Otherwise, that is, if any of the authorities concerned makes a

relevant and reasoned objection to the draft decision, the supervisory authority

principal may follow what is indicated in the objection, presenting the opinion of the other

control authorities concerned a revised draft decision, which will be submitted

to the procedure indicated in section 4 within two weeks. not to follow

indicated in the objection or if it is considered that it is not pertinent, the authority of

main control must submit the matter to the coherence mechanism contemplated in

Article 63 of the GDPR.

In the present case, the AEPD initially estimated that there were no indications of

infraction, for which, on 09/28/2020, a Draft Decision was issued, by means of

which was submitted to the consideration of the rest of the control authorities concerned on

claim file (Draft decision).

At the end of the established period, the

Dutch data protection authority (Autoriteit Persoonsgegevens -AP),

in the sense expressed in the Background of this act.

Taking into account the reasons set out in the objections made, and

in accordance with the provisions of section 1 of article 60 of the RGPD, before

transcribed, which obliges the main supervisory authority to cooperate with the other

authorities, striving to reach a consensus, the procedure was followed

provided for in section 5 of the aforementioned article 60, instead of resorting to the

coherence contemplated in article 63 of the RGPD.

Although this Agency initially considered that there were no indications of infraction, a

Once the observations or objections raised by the supervisory authority have been analyzed

interested party, some circumstances were revealed that had not been

sufficiently valued in the draft file of actions (Draft decision),

which will be exposed in the Foundations of Law that follow.

For this reason, it was appropriate to prepare a Revised Draft Decision that

contemplate the opening of a sanctioning procedure against MARINS PLAYA.

This action is in accordance with the cooperation procedure regulated in article

60 of the GDPR; and takes into account the provisions of article 58.4 of the same

Regulation, according to which the exercise of the powers conferred on the authority of

control must respect the procedural guarantees established in Union law

and of the Member States.

The Spanish procedural regulations, specifically, Law 39/2015, of October 1, of the

Common Administrative Procedure of Public Administrations (LPACAP),

establishes that procedures of a sanctioning nature will always be initiated

ex officio by agreement of the competent body, which must contain, among other

indications, the identification of the person or persons allegedly responsible,

the facts that motivate the initiation of the procedure, its possible qualification and the

penalties that may apply

The adoption of this draft agreement to initiate the sanctioning procedure is provided for in article 64 of the LOPDGDD, sections 2 (third paragraph) and 3, establishing the obligation to give formal knowledge to the interested party. Is notification interrupts the prescription of the infraction.

The Revised Draft Decision prepared by the AEPD, in the form of a draft opening of sanctioning procedure, was submitted to the consideration of the interested authority, in order to formulate the objections that they deem pertinent or give your consent. To do this, it was transmitted through the IMI System to these authorities, letting him know that, in case he did not raise objections in the period of two weeks from the consultation, the mandatory agreement of opening of sanctioning procedure. The interested control authority did not formulate no objection, so it was understood that there was agreement on the aforementioned project.

Consequently, on 07/19/2021, the AEPD agreed to initiate this sanctioning procedure, according to the arguments and accusations contained in the Revised Draft Decision.

On the other hand, section 4 of the aforementioned article 64 of the LOPDGDD establishes that The processing times established in this article will be automatically suspended when it is necessary to collect information, consultation, request for assistance or mandatory pronouncement of a body or agency of the European Union or of a or several control authorities of the Member States in accordance with the provisions in the RGPD, for the time between the request and the notification of the statement to the Spanish Data Protection Agency.

III

Article 6 of the RGPD refers to the "Legality of the treatment" in the terms

following:

Article 6 of the RGPD.

"1. The treatment will only be lawful if at least one of the following conditions is met:

a) the interested party gave his consent for the treatment of his personal data for one or

various specific purposes;

b) the treatment is necessary for the execution of a contract in which the interested party is a party

or for the application at the request of the latter of pre-contractual measures;

c) the treatment is necessary for the fulfillment of a legal obligation applicable to the

data controller;

d) the processing is necessary to protect the vital interests of the data subject or another person

physical;

e) the treatment is necessary for the fulfillment of a mission carried out in the public interest

or in the exercise of public powers conferred on the data controller;

f) the treatment is necessary for the satisfaction of legitimate interests pursued by the

responsible for the treatment or by a third party, provided that said interests are not

prevail the interests or the fundamental rights and freedoms of the interested party that

require the protection of personal data, in particular when the interested party is a child.

The provisions of letter f) of the first paragraph shall not apply to the treatment carried out by

public authorities in the exercise of their functions.

2. Member States may maintain or introduce more specific provisions in order to

adapt the application of the rules of this Regulation with regard to the treatment in

compliance with section 1, letters c) and e), establishing more precise requirements
specific treatment and other measures that guarantee lawful and fair treatment, with
inclusion of other specific situations of treatment under chapter IX.

3. The basis of the treatment indicated in section 1, letters c) and e), must be established by:

a) Union law, or

b) the law of the Member States that applies to the data controller.

The purpose of the treatment must be determined in said legal basis or, as regards
to the treatment referred to in section 1, letter e), will be necessary for the fulfillment of
a mission carried out in the public interest or in the exercise of public powers vested in the
responsible for the treatment. Said legal basis may contain specific provisions for
adapt the application of the rules of this Regulation, among others: the conditions
general that govern the legality of the treatment by the person in charge; data types
object of treatment; affected stakeholders; the entities to which they can be communicated
personal data and the purposes of such communication; purpose limitation; the terms of
data conservation, as well as the operations and procedures of the treatment,
including measures to ensure fair and lawful treatment, such as those relating to
other specific situations of treatment under chapter IX. Union law or
of the Member States shall fulfill a public interest objective and shall be proportionate to the end
legitimate persecuted.

4. When the treatment for another purpose other than that for which the data was collected
personal information is not based on the consent of the interested party or on Union Law or
of the Member States which constitutes a necessary and proportionate measure in a society
democracy to safeguard the objectives indicated in article 23, paragraph 1, the
data controller, in order to determine whether processing for another purpose is
compatible with the purpose for which the personal data was initially collected, will take into account
account, among other things:

a) any relationship between the purposes for which the personal data was collected and

the purposes of the intended further processing;

b) the context in which the personal data were collected, in particular with regard to

to the relationship between the interested parties and the data controller;

c) the nature of the personal data, specifically when dealing with special categories

of personal data, in accordance with article 9, or personal data relating to convictions

and criminal offenses, in accordance with article 10;

d) the possible consequences for data subjects of the envisaged further processing;

e) the existence of adequate guarantees, which may include encryption or pseudonymization".

It takes into account what is expressed in recitals 40 to 45 and 47 of the RGPD in

in relation to the provisions of articles 6 and 7 of the GDPR outlined above.

In the present case, a claim is made against the entity MARINS PLAYA for

perform, during the process of registering the claimant in the hotel, a digital scan

of his passport, of the entire document, despite the opposition expressed by the

same; as well as for the use of the personal data contained in the aforementioned

document, including a photograph, for the control and invoicing of the consumption of the

client during their stay.

The actions carried out have made it possible to verify that the scanning process

to which the client's identification document is submitted upon arrival at the hotel does not have

in order to obtain a digital image of the entire document. As detailed

in Proven Fact 2, said scanning is carried out using a computer program

Optical Character Recognition (OCR) that automatically identifies

characters of a certain alphabet and stores them as data, that is,

convert the image to text. It is a support program that captures the data

of the client, integrates them into the entity's information system and enables the

Completion of the "client file" or "passenger entry part".

There is no proof that the responsible entity has an image

Complete identity document of the clients. Nor is it known that the image

A scan of this document is incorporated into the devices used by the staff

of hotel services (bar and dining room).

If it is accredited, on the other hand, and this has been recognized by the MARINS entity itself

PLAYA, which through that process the aforementioned entity collects the personal data of

your clients regarding the number, type and date of issue of the identity document

presented, name and surname, sex, date and country of birth, as well as the

Photography; and that they are sent to the State Security Forces and Bodies in

compliance with citizen security regulations and used for the "management

hotel", according to the terms used by the entity itself in its response to the

AEPD Inspection Services.

This includes the use of personal data by the administration staff and

of services. According to the documentation provided by the claimed entity, the staff

of services uses a device that has incorporated information regarding the

clients, which includes the room and reservation number, number of people and

departure date; name and surname of the person, status, type of VIP and number of

visits, in addition to the photograph of the client, which is checked to verify the

identity of the client when making consumptions in the hotel; but they don't have the

scanned image of the identity document.

The data collected, except for the photograph, are necessary for the execution of the

contract in which the interested party is a party and for the fulfillment of an obligation

law applicable to the data controller. Therefore, the treatment of these data

It is protected by the provisions of article 6.1, letters b) and c), of the RGPD.

The regulations that regulate the books-records and parts of entry of travelers in

hotel establishments, as well as the obligation to communicate the information

contained in the registration sheets to the police agencies, is constituted,

Basically, by Organic Law 4/2015, of March 30, on the protection of the

citizen security, and Order INT/1922/2003, of July 3, on registry books and

parts of entry of travelers in hotel establishments and other analogous.

Article 24 of Organic Law 4/2015 provides in its first section the following:

“Individuals or legal entities that carry out activities relevant to the security

citizen, such as lodging ... will be subject to registration obligations

documentation and information in the terms established by the provisions

applicable”.

This rule, and the aforementioned Order, in which those obligations are detailed,

legitimizes the collection of personal data related to the document number of

identity, type of document and date of issue, name and surname, sex, date

of birth and country of nationality, date of entry and signature of the traveler; which

must be incorporated into the "Registration sheet" that the entity responsible for the hotel must

transfer to the State Security Forces and Bodies.

It remains, therefore, to determine the scope that should be granted, from the point of view of

the protection of personal data, the collection and use of photographs of

clients carried out by MARINS PLAYA.

On this issue, the first thing to note is that the information on

protection of personal data that the claimed entity provided to customers not

included no details about the collection and use of the photograph, so they were

unknown to those interested. In fact, not even the data processing to which

The photograph is submitted and appears in the Registry of Treatment Activities.

Therefore, what MARINS PLAYA stated in its letter of

allegations to the motion for a resolution when it points out that the clients were

informed during the registration process at the hotel establishment. It is true that

With this pleadings brief, it has provided an informative document that does

reference to the registration of the photograph in the entity's systems, but it has not

accredited the delivery of this document to clients and has not justified

When did you implement its use?

In this regard, it is interesting to note that in the evidence phase of the procedure the

The instructor expressly required the respondent entity to copy its policy on

privacy, in all its versions effective as of 05/25/2018 and any notice

of privacy or additional information, as well as a detail about the channels

empowered to disclose this information, and said entity did not provide the

informative document that now contributes with its allegations to the proposal of

resolution.

In relation to the photographs of the clients, MARINS PLAYA has stated that

This image is used to make it easier for hotel staff to identify the client.

that you are using the credit or room card (at the time of making

a consumption, the client provides that card to the employee, who, when passing it to carry out the

charge, you can check the photo), as well as to control access to the

establishment. When the customer registers, he is provided with a magnetic card

that allows you, in addition to access to the room, the payment of consumption with charge

to your account, which will be paid at the end of your stay. At the time of making a

consumption, the customer provides that card to the employee, who, by swiping it through his device

to charge, view the customer's photo.

The collection and use of customer photographs are not covered by

the legal bases indicated above (execution of the contract and fulfillment of a

legal obligation).

According to MARINS PLAYA, the aim is to verify the identity of the client in order to avoid

fraudulent use of the card by third parties and prevent causing serious damage

economical to the customer; that expenses are not paid with a lost card that is not

corresponds to the user of the service. Based on this, the aforementioned entity considers that

This treatment is covered by the provisions of article 6.1.f) of the RGPD, since

there is a legitimate interest of the person in charge in charging the true user of the service and

of the client, avoiding the use of the cards in a fraudulent way and that they are loaded

in the accounts of some customers the consumption made by third parties.

The existence of a legitimate interest of the responsible entity and of the

client as a legal basis that provides coverage for the treatment of the photograph of the

customers.

In relation to the legal basis of legitimate interest, article 6 cited establishes:

"1. The treatment will only be lawful if at least one of the following conditions is met:

f) the treatment is necessary for the satisfaction of legitimate interests pursued by the
responsible for the treatment or by a third party, provided that said interests are not
prevail the interests or the fundamental rights and freedoms of the interested party that
require the protection of personal data, in particular when the interested party is a child...".

Recital 47 of the RGPD specifies the content and scope of this base
legitimizer of the treatment:

"(47) The legitimate interest of a controller, including that of a controller to whom
may communicate personal data, or of a third party, may constitute a legal basis
for treatment, provided that the interests or the rights and freedoms of the user do not prevail.
data subject, taking into account the reasonable expectations of data subjects based on their
relationship with the person in charge. Such legitimate interest could occur, for example, when there is a
relevant and appropriate relationship between the data subject and the controller, such as in situations where
which the interested party is a client or is at the service of the person in charge. In any case, the
existence of a legitimate interest would require careful assessment, even if a
The interested party can reasonably foresee, at the time and in the context of the collection of
personal data, which may be processed for this purpose. In particular, the interests and
the fundamental rights of the interested party could prevail over the interests of the
responsible for the treatment when proceeding to the treatment of personal data in
circumstances in which the data subject does not reasonably expect that a
further treatment. Since it is up to the legislator to establish by law the legal basis for
the processing of personal data by public authorities, this legal basis does not
should apply to processing carried out by public authorities in the exercise of their duties.
functions. The processing of personal data strictly necessary for the
prevention of fraud also constitutes a legitimate interest of the data controller.
that it is The processing of personal data for direct marketing purposes may
be considered carried out for legitimate interest".

The interpretative criteria that are extracted from this Considering are, among others, (i)
that the legitimate interest of the person in charge prevails over the interests or rights and
fundamental freedoms of the owner of the data, in view of the expectations
reasonable that he has, based on the relationship he maintains with the person in charge
of the treatment; (ii) it will be essential to carry out a "meticulous evaluation" of
the rights and interests at stake, also in those cases in which the
interested party can reasonably foresee, at the time and in the context of the
data collection, which may be processed for this purpose; (iii) interest and
fundamental rights of the owner of the personal data could prevail against
the legitimate interests of the person in charge when the processing of the data is carried out
in such circumstances in which the data subject "does not reasonably expect"
carry out further processing of your personal data.

MARINS PLAYA has not justified this legitimate interest sufficiently to
allow the weighting test between the interest of the person in charge and the rights of the
interested, necessary to determine the legality of the treatments carried out. In
In this case, moreover, there is no evidence that the aforementioned entity has carried out this test of
weighting and has duly informed the claimant on this basis
legitimizing.

During the test phase of the procedure, the instructor expressly requested the
requested to provide a "Copy of the documents in which the evaluation
carried out on the prevalence or not of the interests and fundamental rights of the

clients against the interests of MARINS PLAYA, in relation to the operations of

processing of personal data of clients carried out under the responsibility of

MARINS PLAYA with which the satisfaction of legitimate interests is intended

persecuted by the MARINS PLAYA entity itself or by a third party". this entity

responded to the agreed request for evidence, but did not provide any documentation

regarding the processing of personal data based on legitimate interest.

The respondent entity did not carry out this prior analysis, although it refers to it in its

writing of allegations to the proposal, and at no time informs the clients

on this legal basis of the treatment. About the informative document provided with

said letter of allegations, which contains a reference to the legitimate interest, we

We refer to what was indicated above about said informative writing.

In the absence of information regarding the weighting test, the interested party is deprived

of their right to know the legal basis of the treatment alleged by the person in charge, and

specifically, when referring to the legitimate interest, he is deprived of his right to know

what are said legitimate interests alleged by the person in charge or by a third party that

would justify processing without taking your consent into account.

In the same way, the interested party is deprived of his right to claim for what reasons

Said legitimate interest alleged by the person in charge could be counteracted by the

rights or interests of the interested party. Not having given the interested party an opportunity

to allege them against the person in charge, any weighing carried out by the person in charge

without taking into account the circumstances that the interested party could allege, to whom it was not

allowed to do so would be vitiated, as it is an act contrary to a mandatory norm.

It is difficult to accept that a treatment is based on the legitimate interest of the controller

when that treatment is carried out in a hidden way.

It is not possible, therefore, to invoke this legal basis of legitimate interest on the occasion of a

administrative procedure, such as transfer of the claim or allegations to the

opening of the sanctioning procedure. Accepting it would be the same as admitting an interest

legitimate supervening, or a posteriori, in respect of which the

requirements set forth in the personal data protection regulations and on which

stakeholders are not informed.

Although the legitimate interest is not applicable, it is interesting to analyze the terms in which it must

carry out the weighting provided for in article 6.1.f) of the RGPD between the legitimate

interest of the person responsible for the data and the protection of personal data of the

interested, that is, how it plays said legitimate interest, if applicable.

The CJEU, in its ruling of 05/04/2017, C-13/16, Rigas Satskime, sections 28 to 34,

determined what are the requirements for a treatment to be lawful on

the basis of legitimate interest. The CJEU ruling of 07/29/2019, C-40/17, Fashion ID,

Echoing the sentence cited, it collects said requirements.

28. In this regard, article 7, letter f), of Directive 95/46 -(current article 6.1.f) of the RGPD)-

sets three cumulative requirements for the processing of personal data to be lawful:

first, that the data controller or the third party or third parties to whom they are communicated

the data pursues a legitimate interest; second, that the treatment is necessary for the

satisfaction of that legitimate interest and, third, that the rights and freedoms

fundamentals of the interested party in the protection of data.

This legal basis requires the existence of real interests, not speculative and that,

Also, they are legitimate. And not only does the existence of that legitimate interest mean that

those treatment operations can be carried out. It is also necessary that these

treatments are necessary to satisfy that interest and consider the repercussion
for the interested party, the level of intrusion on their privacy and the effects that may
negatively impact it.

Regarding the first of the requirements, that is, that the data controller or
third parties pursue a legitimate interest, such as preventing fraudulent use of the card
that the claimed delivery to its customers, we are faced with an interest that could
considered legitimate in itself, although said interest must be weighed against the
of the individuals. That is, even if the person in charge has said legitimate interest, this
does not mean, in itself considered, that this basis can simply be invoked
legal as a basis for processing. The legitimacy of this interest is only a
starting point, only one of the elements to be weighed.

Regarding the second of the requirements, however, it is considered that the treatment
of personal data carried out by MARINS PLAYA is not necessary or strictly
necessary for the satisfaction of the alleged legitimate interest (the cited judgment of
05/04/2017, C-13/16, Rigas Satskime, in its section 30, declares “As regards the
requirement that data processing is necessary, it should be remembered that the
exceptions and restrictions to the principle of protection of personal data
personnel must be established without exceeding the limits of what is strictly
necessary").

This principle, according to which the treatment must be strictly necessary for the
satisfaction of legitimate interest, it must be interpreted in accordance with what
established in article 5.1.c) RGPD, which refers to the principle of
data minimization, noting that personal data will be “adequate,
relevant and limited to what is necessary in relation to the purposes for which they are
treaties”.

Thus, less invasive means of serving a patient should always be preferred.

same end. Necessity implies here that the treatment is essential for the

satisfaction of said interest, so that, if said objective can be achieved

reasonable manner in another manner that is less impactful or less intrusive, the

Legitimate interest cannot be invoked.

The term “necessity” used in article 6.1 f) of the RGPD has, in the opinion of the CJEU, a

own and independent meaning in Community law. It's about a

“autonomous concept of Community Law” (STJUE of 12/16/2008, case C-

524/2006, section 52). On the other hand, the European Court of Human Rights

(ECHR) has also offered guidelines to interpret the concept of necessity. In

its Judgment of 03/25/1983 specified that, without prejudice to the treatment of the

data of the claimants is "useful", "desirable" or "reasonable", as specified by the ECHR in

its Judgment of 3/25/1983, the term “necessary” does not have the flexibility that is

implicit in those expressions.

The more "negative" or "uncertain" the impact of treatment may be, the more

It is unlikely that the processing as a whole can be considered legitimate.

As can be seen, what was stated above is in line with the doctrine of

Constitutional Court on the proportionality trial that must be carried out on

a restrictive measure of a fundamental right. According to this doctrine, they should

three requirements must be verified: suitability (if the measure allows the objective

proposed); necessity (that there is no other more moderate measure); proportionality in

strict sense (more benefits or advantages than harm).

In short, leaving aside the fact that the interested party does not know for what purposes or on what legal basis your data has been collected, it is understood that the collection and use of the photograph of the clients that MARINS PLAYA carries out supposes a excessive processing of personal data.

In relation to this question, all the arguments put forward by the data protection authority of the Netherlands, outlined in the Background

Fourth, to challenge the processing of said personal data under the established in article 6.1.f) of the same RGPD, considering that there are other Less intrusive ways to verify if the magnetic card holder is the legitimate one holder of the same at the time of payment and, thus, prevent said cards from being used fraudulently.

On the other hand, the proceedings do not show that MARINS PAYA has established additional guarantees that could favor the acceptance of this base legal data processing, such as favoring the right of opposition of the interested party or even establish voluntary exclusion mechanisms.

In short, the legitimate interest invoked by MARINS PLAYA does not prevail against the fundamental rights and freedoms of those interested in the protection of their data personal, so it cannot be considered that the processing of personal data that carried out is protected by the legitimate interest provided for in article 6.1.f) of the GDPR.

Nor does the interested party give their consent for said data processing. Of In accordance with what is expressed in the aforementioned regulations, the data processing object of the claim require the existence of a legal basis that legitimate, such as the consent of the interested party validly given, necessary

when there is no other legal basis mentioned in article 6.1 of the

RGPD or the treatment pursues a purpose compatible with that for which they were collected

the data.

Article 4 of the GDPR defines "consent" in the following terms:

“Article 4 Definitions

For the purposes of this Regulation, the following shall be understood as:

11. «consent of the interested party»: any manifestation of free will, specific,

informed and unequivocal by which the interested party accepts, either by means of a declaration or a

clear affirmative action, the treatment of personal data that concerns you”.

In relation to the provision of consent, what is established in the

article 6 of the RGPD, already mentioned, and in articles 7 of the RGPD and 7 of the LOPDGDD.

Article 7 “Conditions for consent” of the RGPD:

"1. When the treatment is based on the consent of the interested party, the person in charge must

be able to demonstrate that they consented to the processing of their personal data.

2. If the data subject's consent is given in the context of a written statement that

also refers to other matters, the request for consent will be presented in such a way

clearly distinguishable from other matters, in an intelligible and easily accessible manner and

using clear and simple language. No part of the declaration will be binding.

constitutes an infringement of this Regulation.

3. The interested party shall have the right to withdraw their consent at any time. The retreat

of consent will not affect the legality of the treatment based on the consent prior to

his withdrawal. Before giving their consent, the interested party will be informed of it. it will be so easy

Withdraw consent as give it.

4. When assessing whether consent has been freely given, it will be taken into account to the greatest extent possible whether, among other things, the performance of a contract, including the provision of a service, is subject to consent to the processing of personal data that are not necessary for the execution of said contract".

Article 6 "Treatment based on the consent of the affected party" of the LOPDGDD:

"1. In accordance with the provisions of article 4.11 of Regulation (EU) 2016/679, consent of the affected party means any manifestation of free will, specific, informed and unequivocal by which it accepts, either through a statement or a clear affirmative action, the treatment of personal data that concerns you.

2. When the data processing is intended to be based on the consent of the affected party for a plurality of purposes it will be necessary to state specifically and unequivocally that said consent is granted for all of them.

3. The execution of the contract may not be subject to the affected party consenting to the treatment of personal data for purposes that are not related to the maintenance, development or control of the contractual relationship".

Consent is understood as a clear affirmative act that reflects a free, specific, informed and unequivocal manifestation of the interested party's accept the treatment of personal data that concerns you, provided with sufficient guarantees to prove that the interested party is aware of the fact that you give your consent and the extent to which you do so. And it must be given to all treatment activities carried out with the same or the same purposes, so that, when the treatment has several purposes, consent must be given for all

them in a specific and unequivocal manner, without the execution of the
contract that the affected party consents to the processing of their personal data for
purposes that are not related to the maintenance, development or control of the
business relationship. In this regard, the legality of the treatment requires that the interested party be
informed about the purposes for which the data is intended (consent
informed).

Consent must be given freely. It is understood that consent
is free when the interested party does not enjoy true or free choice or cannot
deny or withdraw your consent without prejudice; or when you don't know
allows separate authorization of the different data processing operations
despite being appropriate in the specific case, or when the fulfillment of a
contract or provision of service is dependent on consent, even when it
not necessary for such compliance. This occurs when consent is
included as a non-negotiable part of the general conditions or when
imposes the obligation to agree to the use of additional personal data to
those strictly necessary.

Without these conditions, the provision of consent would not offer the data subject a
true control over your personal data and its destination, and this would
Illegal treatment activity.

The Article 29 Working Group analyzed these issues in its document
“Guidelines on consent under Regulation 2016/679”, revised and
approved on 04/10/2018; which has been updated by the European Committee for
Data Protection on 05/04/2020 through the document “Guidelines 05/2020 on
consent in accordance with Regulation 2016/679”. From what is stated in this
document, it is now interesting to highlight some aspects related to the validity of the

consent, specifically on the elements “specific”, “informed” and

"unequivocal":

“3.2. Specific declaration of will

Article 6, paragraph 1, letter a), confirms that the consent of the interested party for the

processing of your data must be given "for one or more specific purposes" and that an interested party

may choose with respect to each of such purposes. The requirement that consent

should be 'specific' is intended to ensure a level of control and transparency for the

interested. This requirement has not been changed by the GDPR and remains closely

linked to the requirement of “informed” consent. At the same time, it must be interpreted

in line with the “dissociation” requirement to obtain “free” consent. In sum,

In order to comply with the “specific” character, the data controller must apply:

i) specification of the purpose as a guarantee against deviation from use,

ii) dissociation in consent requests, and

iii) a clear separation between information related to obtaining consent

for data processing activities and information relating to other matters.

Ad. i): In accordance with article 5, paragraph 1, letter b), of the RGPD, obtaining the

Valid consent is always preceded by the determination of a specific, explicit and

legitimate for the intended treatment activity. The need for specific consent

in combination with the notion of purpose limitation in Article 5, paragraph

1, letter b), works as a guarantee against the gradual expansion or blurring of the purposes

for which the data processing is carried out once an interested party has given their

Authorization for the initial data collection. This phenomenon, also known as

deviation of the use, supposes a risk for the interested parties since it can give rise to a use

unforeseen personal data by the data controller or third parties

parties and the loss of control by the interested party.

If the data controller relies on Article 6(1)(a), the data subjects

They must always give their consent for a specific purpose for data processing.

In line with the concept of purpose limitation, with Article 5, paragraph 1, letter

b), and with recital 32, the consent may cover different operations, provided

that these operations have the same purpose. It goes without saying that the specific consent

can only be obtained when the interested parties are expressly informed about the purposes

provided for the use of data concerning them.

Without prejudice to the provisions on the compatibility of purposes, the consent must

Be specific for each purpose. The interested parties will give their consent on the understanding that they have

control over your data and that these will only be processed for those specific purposes. If a

responsible processes data based on consent and, in addition, wishes to process said data

for another purpose, you must obtain consent for that other purpose, unless there is another basis

law that best reflects the situation...

Ad. ii) Consent mechanisms should not only be separated in order to comply

the requirement of “free” consent, but must also comply with the requirement of

"specific" consent. This means that a data controller seeking the

consent for several different purposes, you must facilitate the possibility of opting for each purpose,

so that users can give specific consent for specific purposes.

Ad. iii) Finally, data controllers must provide, with each data request,

separate consent, specific information on the data to be processed for each purpose,

in order that the interested parties know the repercussion of the different options that

have. In this way, data subjects are allowed to give specific consent. Is

issue overlaps with the requirement that controllers provide clear information, as

as discussed above in section 3.3".

"3.3. Manifestation of informed will

The GDPR reinforces the requirement that consent must be informed. in accordance

with article 5 of the RGPD, the requirement of transparency is one of the principles

fundamental, closely related to the principles of loyalty and legality. To ease

information to the interested parties before obtaining their consent is essential so that they can

make informed decisions, understand what they are authorizing and, for example,

exercise your right to withdraw your consent. If the controller does not provide information

accessible, user control will be illusory and consent will not constitute a valid basis

for data processing.

If the requirements for informed consent are not met, the consent is not

will be valid and the person in charge may be in breach of article 6 of the RGPD.

3.3.1. Minimum content requirements for consent to be "informed"

In order for the consent to be informed, it is necessary to communicate to the interested party certain

elements that are crucial to be able to choose. Therefore, the WG29 is of the opinion that it is required,

least, the following information to obtain valid consent:

i) the identity of the data controller,

ii) the purpose of each of the treatment operations for which the authorization is requested.

consent,

iii) what (type of) data will be collected and used,

iv) the existence of the right to withdraw consent,

v) information on the use of data for automated decisions in accordance with the

article 22, paragraph 2, letter c), when relevant, and

vi) information on the possible risks of data transfer due to the absence of

a decision of adequacy and adequate guarantees, as described in the article

46”.

In the alleged case, there is no evidence of the provision of a

valid consent on the part of MARINS PLAYA clients that protects the

processing of personal data that MARINS PLAYA carries out with the photograph

of these clients. This entity does not even report on this use of the

photography, nor has it established any mechanism so that customers can consent

this use by means of a separate affirmative act for these specific

treatment operations, which are also not included in the Registry of

Treatment Activities.

Consequently, in accordance with the exposed evidence, the aforementioned facts

represent a violation of the provisions of article 6 of the RGPD, which gives rise to the

application of the corrective powers that article 58 of the aforementioned Regulation grants to

the Spanish Data Protection Agency.

As can be seen from the above, the conclusions obtained

on the facts analyzed go beyond the specific action of MARINS

PLAYA regarding the collection and processing of personal data of the claimant, and

have to do with the personal data management process implemented by this

entity in general. Therefore, contrary to what was stated by this entity

in his brief of arguments to the motion for a resolution, it is irrelevant whether the

Whether or not the claimant objected to the delivery of his passport at the time of registration in

the hotel.

It is equally irrelevant that the photograph of the clients is only

view by service personnel. What matters is the treatment that is carried out,

that entails the registration of the photograph in the information systems of the

claimed, and the circumstances in which such registration is carried out.

Finally, it should be noted that the tests completed in the procedure allow

reject the statement made by MARINS PLAYA in its pleadings brief to the

motion for a resolution, on the conservation of the photograph only during the

the client's stay at the hotel and its subsequent elimination. The card itself

claimant, which was required by the instructor, proves that currently his

photograph continues to be preserved in the information system of the claimed person.

IV

In the event that there is an infringement of the provisions of the RGPD, between the

corrective powers available to the Spanish Data Protection Agency,

as a control authority, article 58.2 of said Regulation contemplates the

following:

"two. Each control authority will have all the following corrective powers indicated below:

continuation:

(…)

b) send a warning to any person responsible or in charge of the treatment when the

treatment operations have violated the provisions of this Regulation;

(...)

d) order the person responsible or in charge of the treatment that the treatment operations be

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

manner and within a specified time;

(…)

i) impose an administrative fine under article 83, in addition to or instead of the

measures mentioned in this section, according to the circumstances of each case

particular;".

According to the provisions of article 83.2 of the RGPD, the measure provided for in letter d)

above is compatible with the sanction consisting of an administrative fine.

v

The exposed facts do not comply with the provisions of article 6 of the RGPD, which

involves the commission of an offense classified in section 5.a) of article 83 of the

RGPD, which under the heading “General conditions for the imposition of fines

administrative” provides the following:

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

section 2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a

company, of an amount equivalent to a maximum of 4% of the total annual turnover

of the previous financial year, opting for the highest amount:

a) the basic principles for the treatment, including the conditions for the consent to

tenor of articles 5, 6, 7 and 9”.

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

infractions the acts and behaviors referred to in sections 4, 5 and 6 of the

Article 83 of Regulation (EU) 2016/679, as well as those that are contrary to the

present organic law”.

For the purposes of the limitation period, article 72 of the LOPDGDD indicates:

“Article 72. Infractions considered very serious.

1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679, they are considered

very serious and will prescribe after three years the infractions that suppose a violation

substance of the articles mentioned therein and, in particular, the following:

(…)

b) The processing of personal data without the concurrence of any of the conditions of legality of the

treatment established in article 6 of Regulation (EU) 2016/679".

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

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

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

in accordance with this article for the infringements of this Regulation indicated in the

sections 4, 9 and 6 are in each individual case effective, proportionate and dissuasive.

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

individually, in addition to or as a substitute for the measures referred to in article 58,

section 2, letters a) to h) and j). When deciding to impose an administrative fine and its amount

In each individual case, due account shall be taken of:

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

scope or purpose of the treatment operation in question as well as the number of

affected parties and the level of damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the person responsible or in charge of the treatment to alleviate the

damages suffered by the interested parties;

d) the degree of responsibility of the data controller or processor, taking into account

of the technical or organizational measures that they have applied by virtue of articles 25 and 32;

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

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

infringement and mitigate the possible adverse effects of the infringement;

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

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

The person responsible or the person in charge notified the infringement and, if so, to what extent;

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

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

matter, compliance with said measures;

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

approved under article 42, and

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

financial benefits obtained or losses avoided, directly or indirectly, through

the infraction".

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

has:

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of the Regulation (EU)

2016/679 will be applied taking into account the graduation criteria established in the

section 2 of the aforementioned article.

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

may be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of data processing

personal.

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

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

infringement.

e) The existence of a merger by absorption process subsequent to the commission of the infraction,

that cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

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

h) Submission by the person in charge or person in charge, on a voluntary basis, to

alternative conflict resolution mechanisms, in those cases in which there are

controversies between them and any interested party".

In accordance with the precepts indicated, in order to set the amount of the penalty to

impose in the present case, it is considered appropriate to graduate said sanction from

according to the following criteria:

The following graduation criteria are considered concurrent as aggravating:

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

infringement, taking into account the nature, scope or purpose of the operation

of treatment in question as well as the number of interested parties affected and the

level of damages they have suffered.

. In relation to the duration of the infringement, it is stated in the proceedings that the

collection of personal data carried out by the claimed party, which includes the

collection of the client's photograph, there has been at least one

from 08/27/2018, date of entry into the claimant's hotel, and

currently maintains.

. Number of interested parties: the infraction affects all the clients of the

entity.

. The nature of the damage caused to the interested persons, which

have seen increased risk to their privacy.

. Article 83.2.b) of the RGPD: "b) the intention or negligence in the infringement".

It should be noted that the procedure for collecting personal data

implemented by MARINS PLAYA supposes, from the point of view of the

interested holders of the data collected, the loss of the disposition and control

about their data, because they do not even know that this data collection includes

the photograph that appears on the identification document provided by the client to

your arrival at the hotel.

These circumstances, in addition to those meant in the previous section,

revealed the negligent action of MARINS PLAYA. In this regard, it

takes into account what was declared in the Judgment of the National High Court of 10/17/2007

(rec. 63/2006) that, based on the fact that these are entities whose activity has

coupled with the continuous processing of customer data, indicates that "... the Court

Supreme has understood that there is imprudence whenever it is neglected

a legal duty of care, that is, when the offender does not behave with the

due diligence. And in assessing the degree of diligence, it must be weighed

especially the professionalism or not of the subject, and there is no doubt that, in the

case now examined, when the activity of the appellant is constant and

abundant handling of personal data, it must be insisted on the rigor and

exquisite care to adjust to the legal precautions in this regard".

It is a company that processes the personal data of its

clients in a systematic and continuous manner and that extreme care must be taken in the

compliance with its data protection obligations.

In addition, it is considered that he has had knowledge on several occasions, during the

processing of the claim, about the possible irregularity of its action and not

No action has been taken to correct it.

. Article 83.2.d) of the RGPD: “d) the degree of responsibility of the person in charge or of the

data processor, taking into account the technical or organizational measures

that they have applied by virtue of articles 25 and 32”.

The imputed entity does not have adequate procedures in place for

performance in the collection and processing of personal data, so

that the infringement is not the result of an anomaly in the functioning of

these procedures but a defect in the data management system

personal designed by the person in charge.

. Article 83.2.g) of the RGPD: “g) the categories of personal data

affected by the infringement.

Although “Special categories of personal data” have not been affected,

as defined by the RGPD in article 9, this does not mean that the stolen data is not

were sensitive in nature. The personal data affected by the treatment (the

photography of clients) has a particularly sensitive nature, in that

allows the prompt identification of the interested parties and increases the risks on their

privacy, especially when it is registered associated with all the data that

appear on the holder's identity document, as in this case.

. Article 76.2.a) of the LOPDGDD: “a) The continuous nature of the infraction”.

The procedure for collecting and processing personal data implemented by the

claimed applies to all customers during, at least, the period indicated in the

refer to the duration of the infraction. It is a plurality of actions that

follow the action designed by MARINS PLAYA, which violate the same

precept.

. Article 76.2.b) of the LOPDGDD: “b) The link between the activity of the offender

with the processing of personal data”.

The high link between the activity of the offender and the performance of treatment

of personal data, considering the activity carried out in the sector

hotelier and its volume of activity (in the Fifth Antecedent, some

details about it).

. Article 83.2.k) of the RGPD: “k) any other aggravating or mitigating factor

applicable to the circumstances of the case, such as the financial benefits obtained

or losses avoided, directly or indirectly, through the infringement”.

The medium-sized company and business volume of MARINS PLAYA (in

the Fifth Antecedent contains some details in this regard).

It is also considered that there are extenuating circumstances

following:

. Article 83.2.k) of the RGPD: “k) any other aggravating or mitigating factor

applicable to the circumstances of the case, such as the financial benefits obtained

or losses avoided, directly or indirectly, through the infringement”.

Although the collection of personal data related to photography is considered excessive

of the client and the subsequent use that is made of it, is taken into account

the purpose intended by the claimed entity, to avoid fraud in the

consumption of services, and that no other use other than this data has been accredited

staff.

Considering the exposed factors, the valuation reached by the fine, for the

Violation of article 6 of the RGPD, it is 30,000 euros (thirty thousand euros).

It is interesting to note that MARINS PLAYA has not made any allegation regarding

the graduation of the sanction in the brief presented in response to the proposal of

resolution prepared by the instructor of the procedure.

SAW

The infractions committed may lead to the imposition of the person responsible for the

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

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

according to which each control authority may "order the person in charge or in charge

of the treatment that the treatment operations comply with the provisions of the

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

specified period…".

In this case, it is appropriate to require the responsible entity so that, within the term

indicates in the operative part, cessation in the collection and treatment of the photograph of its

customers. In another case, you must adapt the information on data protection

data offered to customers, especially that relating to the collection and use of

the photograph and the legal basis that supports the treatment, establishing

mechanisms that allow proving that said information is accessed by the

interested; and carry out the necessary adaptation of the treatment operations to which this act refers to the requirements contemplated in article 6.1 of the RGPD, with the scope expressed in the previous Legal Foundations.

Likewise, it must correct the effects of the infraction committed, which entails the deletion of all photographs collected from customers in the circumstances that have determined the declaration of the infraction that is sanctioned in this act.

It is warned that not meeting the requirements of this organization may be considered as a serious administrative infraction by "not cooperating with the Authority of control" before the requirements made, being able to be valued such behavior to the time of the opening of an administrative sanctioning procedure with a fine pecuniary

Therefore, in accordance with the applicable legislation and having assessed the criteria for graduation of sanctions whose existence has been proven,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE the entity MARINS PLAYA, S.A., with CIF A07158223, for an infringement of Article 6 of the RGPD, typified in Article 83.5.a) of the RGPD and classified as very serious for prescription purposes in article 72.1.b) of the LOPDGDD, a fine of 30,000 euros (thirty thousand euros).

SECOND: Require the entity MARINS PLAYA, S.A. so that, within a month, adopt the necessary measures to adapt its actions to the regulations of protection of personal data, with the scope expressed in the Foundation of

Right VI. Within the indicated period, the aforementioned entity must justify before this Agency

Spanish Data Protection the attention of this requirement.

THIRD: NOTIFY this resolution to the entity MARINS PLAYA, S.A.

FOURTH: Warn the sanctioned party that he must make the imposed sanction effective once

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

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

Common 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, through its entry, 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, opened on behalf of the Agency

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

Otherwise, it will be collected in the executive period.

Received the notification and once executed, if the date of execution is

between the 1st and 15th of each month, both inclusive, the term to make the payment

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

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

It will be until the 5th of the second following month or immediately after.

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

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the

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

Interested parties may optionally file an appeal for reconsideration before the

Director of the Spanish Agency for Data Protection within a month from

counting 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 in article 46.1 of the aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP, may provisionally suspend the firm resolution in administrative proceedings if the The interested party expresses his intention to file a contentious-administrative appeal. If this is the case, the interested party must formally communicate this fact by writing addressed to the Spanish Agency for Data Protection, presenting it through Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other registers provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the documentation proving the effective filing of the contentious appeal-administrative. If the Agency was not aware of the filing of the appeal contentious-administrative within a period of two months from the day following the notification of this resolution would end the precautionary suspension.

938-231221

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es