File No: PS/00078/2021
IMI Reference: A56ID 56562- Case Register 64833

FINAL DECISION ON PENALTY PROCEEDINGS

Of the proceedings conducted by the Spanish Data Protection Agency and on the basis of the following

FACTS

FIRST: On 08 January 2019, via the Internal Market Information System (hereinafter IMI), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), the purpose of which is to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information, this Spanish Data Protection Agency (AEPD) received a complaint from [redacted] (hereinafter the complainant), a Dutch citizen, with the Data Protection Authority of the Netherlands (Autoriteit Persoonsgegevens -AP). This complaint is transmitted to the AEPD in accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the General Data Protection Regulation or GDPR), taking into account its cross-border nature and that this Agency is competent to act as lead supervisory authority.

The complaint is lodged against MARINS PLAYA, S.A. (hereinafter MARINS PLAYA or the entity complained against), which has its registered office in Spain, for the following reasons:

The complainant indicates that in the hotel registration process it requested the passport, which was scanned digitally, despite his opposition. The client objects to that document being fully scanned on the ground that not all the information contained therein is necessary, to which the hotel employee replied that the scanning was carried out on the instructions of the police. Secondly, he claims to have seen the hotel employees with the photo of the passport on his tablet.

In relation to the issue raised by the complainant, the referring authority asked whether Spanish law actually requires the full scanning of the passport or only some data is necessary to comply with the registration process.

According to the information contained in the IMI system, in accordance with Article 60 of the GDPR, the supervisory authority which communicated the case (Netherlands) has declared concerned in the present proceedings.

SECOND: In the light of the facts set out above, the General Subdirectorate for Data Inspection took steps to clarify them, in accordance with the powers of investigation conferred on the supervisory authorities in Article 57 (1) of the GDPR. In the context of

these actions, a letter of formal notice was sent to the requested entity, which stated as follows:

1. At the time of the customer's entry registration, his passport is scanned with the aim of moving the image into text to incorporate the fields corresponding to the hotel management programme.
2. Only the page where the customer identification is found is scanned: the traveller identification data, including the number, type and date of issue of the identity document presented, name, sex, date and country of birth, as well as the photograph.
3. There are no specific instructions from the State Security Forces on the copying of the above-mentioned document, except for those relating to the sending of information electronically.
4. The information is also used, in the accounts, to generate the corresponding invoices; only administrative accountancy staff can access them.
5. When the customer is registered, he is provided with a magnetic card enabling him, in addition to access to the room, to pay for consumption from his account at the end of his stay; at the time of consumption, the customer provides that card to the employee, who, on passing it to take charge, can check the photograph of the passport. The purpose of this is to verify the identity of the customer in order to prevent fraudulent use of the card by third parties and to prevent serious financial damage to the customer. The photograph can only be seen by the employee who charges, on the TPV tablet.
6. The legislation applicable to the identification of customers in the process of registration or registration with the hotel is Organic Law 4/2015 of 30 March 1995 on the protection of citizens' safety and Order INT/1922/2003 of 3 July 2007.

THIRD: Having reviewed the replies obtained during the preliminary investigation phase, referred to in the previous facts, this Agency considered that the processing of personal data that is the subject of the complaint is legitimate under Article 6 (1) (c) of the GDPR and is proportionate and necessary in accordance with Article 24 of the Spanish Organic Law 4/2015, which provides in its first paragraph: "Natural or legal *persons carrying out activities relevant to public safety, such as accommodation..., shall be subject to the obligations of recording documents and information in accordance with the terms laid down in the applicable provisions."* This is detailed in the aforementioned Spanish Order (Order INT/1922/2003 of 3 July).

Furthermore, it was taken into account that the alleged facts relating to the scanning of all pages of the passport were not established.

Secondly, it was concluded that the processing of personal data consisting of the use of the photograph obtained from the passport for the purpose of verifying the identity of the customer in the consumption which he makes, by making charges to a room account and preventing the fraudulent use of the hotel card by third parties other than the user of the service, is legitimate under Article 6 (1) (f) of the GDPR, since there is a legitimate interest on the part of the hotel in charging the actual user of the service and for the customer, since the cards are not used fraudulently and the consumption made by others is debited from one customer's account.

Consequently, having clarified the doubts raised, it was considered that there were no indications of an infringement and, therefore, on 28 September 2020, a draft decision was issued to discontinue proceedings (Draft decision).

FOURTH: On 10 November 2020, the draft decision was incorporated into the IMI system so that the authorities concerned could make their views known.

At the end of the prescribed period, the Data Protection Authority of the Netherlands (Autoriteit Persoonsgegevens — AP) objected to that draft decision.

As regards the facts, the supervisory authority notes that the complainant stated that the hotel staff had in their device a full copy of their passport (first page), including their photo, and that this differs slightly from what was stated in the draft decision, although it does not change the assessment made on it.

The AP accepts that the processing of personal data contained in the passport (number, type and date of issue of the identity document presented, name, sex, date and country of birth, as well as the photograph) is necessary for compliance with national law and therefore lawful in accordance with Article 6 (1) (c) GDPR, but questions the processing of such personal data under Article 6 (1) (f) GDPR on the grounds of the existence of a legitimate interest of the hotel responsible in preventing fraudulent use of the card it provides to customers, which serves to make consumption in the premises and also as a key to the room; and also of the customer, as it prevents cards from being used fraudulently and being charged for consumption by others.

On this processing of personal data based on legitimate interest, the AP refers to the requirement of necessity, which requires an assessment of the proportionality and subsidiarity of the processing, verifying that such interests cannot reasonably be effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and the protection of personal data guaranteed by Articles 7 and 8 of the Charter. It adds that the Court of Justice of the European Union further stated that the requirement relating to the need for processing must be examined in conjunction with the principle of 'data minimisation' enshrined in Article 5 (1) (c) of the GDPR.

In this case, the AP points out that there are other less intrusive ways to verify whether the holder of the magnetic card is the legitimate cardholder at the time of payment and thus to prevent such cards from being used fraudulently.

As an example of these less intrusive actions, indicates the possibility for the hotel employee, when any consumption occurs, to consult some control data to the customer, such as surname or room number, to verify whether it matches the legitimate card holder; or requiring the signature of a receipt for consumption, which also acts as a barrier for third parties. In the event of loss of the card, the card may be blocked to prevent fraudulent use.

The combination of the above scenarios requires a minimum amount of additional data processing, is less intrusive and complies with the principle of data minimisation. Nevertheless, they make it possible to achieve the interests pursued through common practices in most hotels.

Against this, the additional effectiveness of the use of personal data in the passport to prevent fraud does not outweigh the invasion of data protection.

Such data can be used for identity fraud in the event of a data breach or abuse by hotel employees who have access to it, so that its use is not considered proportionate to prevent possible fraud in the payment of hotel services.

According to the AP, the processing of all such data is contrary to the principle of data minimisation in accordance with Article 5 (1) (c) GDPR, as the processing of only one name and room number is sufficient to effectively minimise fraud. In addition, some of the data categories mentioned above can be considered as special categories of personal data in accordance with Article 9 GDPR, without any of the exceptions of Article 9 (2) GDPR being applicable to this case.

In summary, the AP does not agree that the use of passport data is allowed under Article 6 (1) (f) GDPR in the circumstances indicated. This could lead to the use of passport data by many hotels and similar service providers, a wider use that could lead to identity fraud in cases of data breaches or abuses by hotel employees who have access to them, so that, given the risk to freedoms and rights expressed, it does not consider their use to prevent possible fraud in the payment of hotel services to be proportionate.

If a hotel wishes to process passport data in order to verify the identity of customers during its stay, add AP, the hotel must invoke another ground of Article 6 GDPR, such as consent, or return to the most common practice, as described above.

FIFTH: On 11 May 2021, the General Subdirectorate of Data Inspection accessed the information available on MARINS PLAYA in 'Axesor'. ***That website contains a turnover for the financial year 2018, the last financial year submitted, of 11 001 697 EUR and a profit for the financial year of 1 715 834 EUR. It is also stated that it is a medium-sized enterprise with 102 employees.*** That entity is registered in the code of economic activity corresponding to 'Hotels and similar accommodation'.

According to the information in the Central Commercial Register, the 'subscribed capital' amounts to 30 000 000 EUR.

SIXTH: On 03 June 2021, in accordance with Article 64 (2) (third subparagraph) and (3) of the Spanish LOPDGDD, a draft decision to initiate penalty proceedings was issued on the basis of the complaint received via the IMI system, as set out in the First Fact. This draft takes into account the objections set out in the Fourth Fact (revised draft decision).

In accordance with the procedure laid down in Article 60 of the GDPR, on 25 June 2021, the aforementioned draft to initiate penalty proceedings was sent via the IMI system to the concerned supervisory authorities, informing them that, if no objections were raised within two weeks of the consultation, the necessary agreement to initiate penalty proceedings would be adopted.

The concerned supervisory authorities did not raise any objection to the draft agreement to initiate penalty proceedings adopted by the AEPD, and it is therefore understood that there is agreement on it.

In accordance with Article 64 of the Spanish LOPDGDD, the requested entity was

notified of the draft decision to initiate penalty proceedings.

SEVENTH: On 15 June 2021, this Agency received a letter from the requested entity requesting the closure of the proceedings, in accordance with the following considerations:

1. It describes the procedure followed by the processing of a customer's personal data from the time of arrival at the hotel, pointing out that documentation proving the identity of all persons over the age of 16 who are accommodated on their premises is requested and that they undergo a scanning process for the registration process, which completes the data collection sheet without storing the image of the document in the computer systems.

This is an optical character recognition known as OCR (*Optical Character Recognition*), which makes it possible to digitise texts (the process automatically identifies the characters of a certain alphabet and stores them in data form). According to the entity, this process only applies to the page of the document on which the traveller is identified, collecting the personal data relating to the number, type and date of issue of the document in question (ID card, passport, driving licence, residence permit or identity card), first name, surname, sex, date and country of birth, as well as the photograph. The traveller is then signed on a digital medium via Tablet, which provides information on the rules on the protection of personal data; he/she is provided with an access pass to the rooms, which is also used for the use of hotel services.

The data are processed by administrative and service staff (bar and canteen) to pay for consumption. They are also referred to the State Security Forces and Corps, in compliance with the rules on public safety.

2. It denies that hotel staff had on their device a complete copy of the first page of the complainant's passport, since the only data appearing on the devices used by bar and canteen staff with access to TPV are the room number, departure date, traveller's name and surname, photograph and accommodation regime, necessary to carry out maintenance, development and negotiation control, legitimising the processing. In that regard, it points out that, from the data available on those devices, only the first name, surname and photograph are taken from the check-in).

3. Taking into account the data used to control consumption and prevent the fraudulent use of the facilities, it does not understand the entity to call into question the legitimate interest, especially when the Agency itself accepts the processing of the personal data contained in the passport in order to comply with national legislation, considering it to be lawful in accordance with Article 6 (1) (c) GDPR.

On the less intrusive ways to identify the customer to which the opening agreement refers, points out that requesting the room number or surname is insufficient orally and does not prevent another person from being able to hear and use this data; the same applies to the signature of a receipt, which the employee would not be able to cross-check. It adds that for those reasons the photograph was included in the digital systems of bar and canteen staff as a means of authentication, even when the customer is not in possession of the card because it is forgotten, lost or stolen.

As regards the risks in case of a potential data breach, it warns that the mechanisms set out in the GDPR have been implemented and that employees have entered into a confidentiality contract.

4. The entity does not process special categories of personal data at any time. On that point, it states that the image of the client is only a photograph from which no biometric templates are extracted or used for facial recognition or other specific means. Therefore, the processing it carries out in order to obtain the photograph which it carries out does not comply with the concept of processing of special categories of data (recital 51 and Article 4 (15) of the GDPR).

Consequently, the entity concludes that the processing of the data used to authenticate the identity of the person making a charge does not infringe Article 6 (1) (f) of the GDPR, since it is necessary for the purposes of the legitimate interests pursued by the controller (avoiding damage and claims for undue recoveries), as well as of the data subject (avoiding undue recovery).

It provides a photograph showing the details of the information available on the hotel staff's devices about a particular person: under the heading 'Reservation details' includes the room number, reservation number, number of persons and date of departure; the heading "Components of the reservation" indicates the name of the person, status, type of VIP and number of visits, as well as the photograph of the client.

EIGHT: On 19 July 2021, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against MARINS PLAYA, in accordance with Articles 63 and 64 of Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations ('the LPACAP'), for the alleged infringement of Article 6 of the GDPR, classified in Article 83 (5) (a) of the same Regulation as very serious for the purposes of limitation period in Article 72 (1) (b) of the LOPDGDD; the penalty that may be imposed, taking into account the evidence available at the time of the agreement and without prejudice to the outcome of the proceedings, would amount to a total of 30,000 EUR (thirty thousand euro).

The same decision initiating the procedure stated that the alleged infringement, if confirmed, may lead to the imposition of measures, in accordance with the provisions of Article 58 (2) (d) of the GDPR.

NINTH: Having been notified of the aforementioned decision to initiate proceedings, the entity submitted a letter dated 22 July 2021, in which it again requested that the penalty proceedings be terminated.

In this new letter, it reproduces verbatim its previous arguments, which are set out in the Seventh Fact. It merely adds that recital 47 of the GDPR allows for the processing of personal data necessary for the prevention of fraud on the basis of the legitimate interest of the controller and that an economic deception carried out with the intention of making a profit is regarded as fraud, with which someone is harmed.

TENTH: On 24 August 2021, it is decided to open a period of evidence, taking into account that the complaint lodged, the documents obtained and generated by the General Subdirectorate of Data Inspection and the Inspection Services, and the Report

on Preliminary Inspection Actions, which forms part of file E/01088/2019, were reproduced for the purposes of proof; and by the submissions made by MARINS PLAYA and the accompanying documentation.

It was also agreed to require the entity to provide the following information or documentation:

"(a) Copy of the record of all client personal data processing activities carried out under the responsibility of MARINS PLAYA. Such a record, as referred to in Article 30 of the GDPR, shall be provided in its initial version, together with any additions, modifications or exclusions to the content of the record.

(b) If available, a copy of the assessment (s) of the impact on the protection of personal data relating to any type of processing operations of customers' personal data carried out under the responsibility of MARINS PLAYA which result in a high risk to the rights and freedoms of natural persons.

The initial version of this impact assessment (s) and, where appropriate, details of any changes or updates that may have been made must be provided.

In addition, if there has been a change in the risk posed by the processing operations and if deemed necessary, it must provide the result of the examination that MARINS PLAYA may have carried out to determine whether the processing complies with the data protection impact assessment (Article 35 (11) GDPR).

(c) Copy of the documents containing the assessment carried out as to whether or not the interests and fundamental rights of the customers take precedence over the interests of MARINS PLAYA, in relation to the processing operations of customers' personal data carried out under the responsibility of MARINS PLAYA seeking to satisfy legitimate interests pursued by MARINS PLAYA itself or by a third party.

(D) Copy of data protection information (privacy policy) provided through any channel to that organisation's customers, in its current version and previous versions in force from 25 May 2018, where applicable, with an indication of the period of validity of each version.

If there are addenda or variations, or other privacy notices or additional information, relating to the processing of personal data, copies of all documents used to inform personal data protection other than the privacy policy are requested.

(e) Details of the channels and procedures for making all personal data protection information known to your customers (privacy policy or any other document).

(f) information regarding the channels, mechanisms and methodology used by that organisation to seek acceptance by its customers of the privacy policy or any other document used by that organisation to report on the protection of personal data; and for the provision of the consents provided for in such documents, where appropriate.

(g) Screen images corresponding to all the information recorded in your information system concerning the complainant in the above penalty proceedings.

(h) Details of the software used by that entity for the collection of customers' data by scanning documents and converting them to text.'

In response to this request, we received a letter from the entity accompanied by the

documentation set out below. In that letter, that entity stated that it was unable to provide the print-outs of the bar and canteen tablets with the information on the complainant available on those devices because that information was deleted at the time when the customer made the check-out, nor the access to Wi-Fi, if any, which were deleted after 12 months (Law 25/2007).

The following should be noted from the content of the documentation provided:

1. Record of client personal data processing activities.

. Purpose: accounting, tax and administrative management;
. Category of data subjects: customers and users;
. Types of data: Identity card or TIN, name, postal or electronic address, telephone, image and manual signature;
. Other type of data: personal characteristics, social circumstances, commercial information, transactions of goods and services;
. Disposals: Law enforcement agencies and forces.
. Access to equipment: access via personalised user and password.

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

After analysing the data structure, regulatory compliance, organisation and resources, as well as security by design and by default, it is concluded that *'there are no risks in the resources used'*.

3. Data protection information (privacy policy) provided via the requested organisation's website.

(a) It provides a copy of the 'Record sheet', which includes a section on establishment and one on 'traveller's details' (identity card number, type of document and date of issue, name, surname, sex, date of birth, country of nationality, date of entry and signature of the traveller). This 'Leaflet' includes an information legend on the protection of personal data, detailing, inter alia, the identity of the controller, the purpose for which the data will be processed, the absence of data communications except for legal obligations, the rights of the data subject, the manner in which the data subject can be exercised and the possibility of lodging a complaint with the AEPD.

An update to this "Registration Sheet" (2019), which contains a new information clause, is attached. This report provides information on the collection and processing of data for the purpose of prevention, investigation, detection or prosecution of criminal offences under Spanish Organic Law 4/2015 of 30 March 1995 on the Protection of Citizens' Safety; whereas the data will be kept for three years and made available to the law enforcement authorities; data subjects' rights and how to exercise them and the possibility to complain to the AEPD.

In addition, the entity provides a copy of the data protection policy available on its website. It is divided into two parts, called *'Privacy Policy'* and *'Second Layer Clauses'* (the latter part is divided into headings: customer file reservation, invoices/accounts, newsletter, web users, employees, etc.).

The *'Privacy Policy' section* refers to personal data collected from customers *'for the purpose of providing them with contracted services consisting of booking hotel accommodation'*.

In the *'Second layer'* information, under the heading *'Reservation account'*, it is stated that the entity deals with the information provided by customers *'in order to provide them with the service and to sell the products requested to them, to charge it and to manage the sending of information and commercial prospecting'*.

In this information, there is no indication of the use of the customer's photograph to control consumption and prevent fraudulent use of the premises.

4. Screenshot corresponding to the information recorded concerning the complainant (data during the check-in). It is presented under the *heading 'Customer file data load'* and includes fields relating to name, surname, document number and date of issue, nationality, date of birth, last visits and photograph. According to this information, the entry to the complainant's hotel took place on 27 August 2018.

5. Details of the software (***'HOTEC PMS HOTEL'***) used for the collection of customers' data by scanning documents and converting them to text, provided by the software developer:

'Procedure for capturing customer data by scanning documents.
At the time of entry to the hotel, your ID/PASAPORT is requested from the client in order to scan this document. In this scanning, the data are captured and integrated into the database by means of an OCR (company...) process, since they are necessary to complete 2 documents essential to the normal functioning of the hotel:

1. Fill in the passenger entry part. This data will be collected and processed in accordance with Regulation (EU) 2016/679 of 27 April (GDPR) and Organic Law 3/2018 of 5 December (LOPDGDD) for the purpose of prevention, investigation, detection or prosecution of criminal offences, and in accordance with Article 25 (1) of Organic Law 4/2015 of 30 March on the Protection of Citizens' Safety.
2. Issuing of billing for hotel expenses.

The image with the customer's photo is captured and saved to secure the customer credit process in the different departments as it makes it easier for hotel staff to identify the customer who is using the credit card or room. It also makes it possible to identify that customer by hotel staff when controlling access to the premises'.

ELEVENTH: On 29 November 2021, a proposal for a resolution was made as follows:

1. That the Director of the Spanish Data Protection Agency penalises MARINS PLAYA for an infringement of Article 6 of the GDPR, defined in Article 83 (5) (a) of the GDPR and classified as very serious for the purposes of limitation in Article 72 (1) (b) of the LOPDGDD, with a fine of 30,000 EUR (thirty thousand euros).

2. That Director of the Spanish Data Protection Agency imposes on MARINS PLAYA, S.A., within a period to be determined, the adoption of the necessary measures to bring its action into line with the legislation on the protection of personal data, with the scope set out in the Legal Grounds VI of the aforementioned proposal for a resolution.

TWELFTH: Having been notified of the aforementioned proposal for a resolution, on 15 December 2021 a letter was received from the entity in which it reiterated its request for closure of the proceedings. The request was based on the following arguments:

1. The complainant, during the registration process at the hotel establishment, which took place on 27 August 2018, three months after the entry into force of the GDPR, provided his passport without showing any opposition. At that time, he was informed of the matters imposed by the GDPR by means of an information document drafted in Spanish and had at his disposal a display with an information clause relating to the data processing carried out. Currently, this information is provided in the most common languages among the entity's customers.

2. Recital 47 of the GDPR expressly states that the processing of personal data which is strictly necessary for the prevention of fraud is also a legitimate interest of the controller, which operates *'ex lege'* where the processing is for that purpose and the parameters to be taken into account in order to carry out the balancing exercise are satisfied, such as whether the data subject is a client or a service, the carrying out of a preliminary analysis and that the processing does not take place in circumstances where the data subject does not expect further processing to be carried out (the perspective of the data subject).

In this case, the first aspect is given; the second was analysed when the technological solution for the check-in was put in place, with the conclusion that it was necessary to inform, limit access to the image exclusively to consumer collection operators and retain the data only during the customer's stay; in addition, image identification has been favourably assessed by customers, as they have avoided erroneous charges, especially when *'all-inclusive'* stays are offered.

3. There are no alternatives that offer the same guarantee by minimising the processing of personal information.

It reiterates that the proposals of the Dutch Data Protection Authority on other less intrusive practices, such as consulting the data subject with certain data (surname or room number) or signing a receipt, are not effective or involve the processing of other data, such as signature, which are not less protective.

4. The image of the customer is only displayed by staff dealing with consumer payments, who subscribe to a confidentiality document, no further processing of that image is carried out and is removed at the end of the customer's stay.

5. The argument put forward by the entity is that which the Agency itself maintained when it initially considered that there were no indications of an infringement.

In its written pleadings, MARINS PLAYA provided a copy of the information document referred to in its submissions. This document explains the process of checking in and processing the image of the identification document by means of a character recognition program. In relation to the photograph, the following is stated:

'The photo on the passport or ID card you provided for the check-in will also be recorded in the hotel management system of the receiving hotel. The purpose is to enable hotel staff to identify you as a housed customer and to control the cost of their consumption during their stay in their room. This photo will be deleted at the time of the check-out.

This processing is based on our legitimate interest in identifying clients accommodated for security and charge control purposes. In weighing this interest against your rights and freedoms, it has been established that the processing had a limited impact on your privacy, as:
— There is a contractual relationship and the processing is carried out in connection with that relationship;
— This security measure benefits the customers themselves by ensuring that charges are properly charged to their room and avoiding possible subplantations;
— Access to your image is restricted to hotel staff;
— The retention period for your image is limited to the length of your stay'.

The actions taken in these proceedings and the documentation contained in the file have shown the following:

PROVEN FACTS

1. MARINS PLAYA provides hotel services and similar accommodation.

2. To register clients (check-in), upon arrival at the hotel, it requests the identification documentation and submit it to a scanning process that makes it possible to digitise texts (the process automatically identifies the characters of a given alphabet and stores them in the form of data), using optical character recognition (OCR) software. This process converts the image into text and incorporates the data into the hotel management programme by filling in the *'customer fiche'* or *'passenger entry part'*, with fields relating to the number, type and date of issue of the submitted identity document, name, sex, date and country of birth. This process applied by the entity also incorporates the customer's photograph into its database.

At this point in time, the customer is provided with a magnetic card which he/she can use both for access to the room and for making use of hotel services.

3. The data collected from the client by MARINS PLAYA are processed by administrative and service staff (bar and canteen); they are referred to the State Security Forces and Corps, in compliance with the rules on public safety.

Service staff use a device that incorporates customer information: under the *heading 'Reservation details'* includes the room number, reservation number, number of persons and date of departure; the heading *'Components of the reservation'* indicates the name of the person, status, type of VIP and number of visits, as well as the photograph of the client.

MARINS PLAYA has stated that the image with the customer's photo is used to provide hotel staff with the identification of the customer who is using the credit card or room (at the time of consumption, the customer provides the card to the employee, who, on passing it to make the charge, can check the photograph), as well as to control access to the establishment.

4. The Record of Processing Activities (RAT) provided by MARINS PLAYA contains the

following information on the processing of personal data of clients:

. Purpose: accounting, tax and administrative management;
. Category of data subjects: customers and users;
. Types of data: Identity card or TIN, name, postal or electronic address, telephone, image and manual signature;
. Other type of data: personal characteristics, social circumstances, commercial information, transactions of goods and services;
. Disposals: Law enforcement agencies and forces.
. Access to equipment: access via personalised user and password.

5. MARINS PLAYA stated during the procedure that, following the scanning of the customer identification document, carried out during the registration process, the traveller's signature is obtained on a digital medium via Tablet, which provides information on the rules on the protection of personal data.

MARINS PLAYA has provided a copy of the *'Record sheet'*, which includes a section on establishment and one on 'traveller's details' (identity card number, type of document and date of issue, name, surname, sex, date of birth, country of nationality, date of entry and signature of the traveller). This *'Leaflet'* includes an information legend on the protection of personal data, detailing, inter alia, the identity of the controller, the purpose for which the data will be processed, the absence of data communications except for legal obligations, the rights of the data subject, the manner in which the data subject can be exercised and the possibility of lodging a complaint with the AEPD.

There is also an update of this *'Registration Sheet'* (2019), which contains a new information clause. This report provides information on the collection and processing of data for the purpose of prevention, investigation, detection or prosecution of criminal offences under Organic Law 4/2015 of 30 March 1995 on the Protection of Citizens' Safety; whereas the data will be kept for three years and made available to the law enforcement authorities; data subjects' rights and how to exercise them and the possibility to complain to the AEPD.

6. MARINS PLAYA have provided the actions with the details of the data protection information (privacy policy) provided through their website. In this information, there is no indication of the use of the customer's photograph to control consumption and prevent fraudulent use of the premises.

7. The complainant's personal data are recorded in the MARINS PLAYA Information System. It is presented under the *heading 'Customer file data load'* and includes fields relating to name, surname, document number and date of issue, nationality, date of birth, last visits and photograph. According to this information, the entry to the complainant's hotel took place on 27 August 2018.

LEGAL GROUNDS

I

By virtue of the powers conferred on each supervisory authority by Article 58 (2) of the GDPR, and in accordance with Articles 47, 64.2 and 68.1 of the Spanish LOPDGDD, the

Director of the Spanish Data Protection Agency is competent to initiate this procedure.

Article 63.2 of the Spanish LOPDGDD states that: *'The procedures handled by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, of this organic law, by the regulatory provisions dictated in their development and, insofar as they are not contradicted, alternatively, by the general rules on administrative procedures'.*

Paragraphs (1) and (2) of Article 58 GDPR list, respectively, the investigatory and corrective powers that the supervisory authority may have for that purpose, by mentioning in point 1 (d) the *power to 'notify the controller or processor of an alleged infringement of this Regulation*'; and in paragraph 2. (i), '*to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case'*.

The case under consideration is based on a cross-border complaint to the Dutch Data Protection Authority (Autoreit Persoonsgegevens -AP) against MARINS PLAYA, which is based in Spain. This is the principal establishment of that entity, within the meaning of the definition in Article 4 (16) of the GDPR. Thus, in accordance with Article 56 (1) GDPR, the AEPD is competent to act as lead supervisory authority.

The following *'definitions'* set out in Article 4 GDPR are taken into account:

'(16) main establishment:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.'

'(21) supervisory authority: the independent public authority which is established by a Member State pursuant to Article 51.'

'(22) supervisory authority concerned: the supervisory authority which is concerned by the processing of personal data because:
A.- The controller or processor is established on the territory of the Member State of that supervisory authority;
B.- Data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing, or
C.- A complaint has been lodged with that supervisory authority.'

'(23) cross-border processing:
(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State;
or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.'

According to the information contained in the IMI system, in accordance with Article 60 of the GDPR, the personal data protection authority of the Netherlands (Autoriteit Persoonsgegevens -AP) acts as *the 'supervisory authorities concerned*' in the present

proceedings.

II

Article 56 (1) of the GDPR, *on 'Competence of the lead supervisory authority*', provides:

'1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure set out in Article 60'.

Article 60 *governs 'Cooperation between the lead supervisory authority and the other supervisory authorities concerned*':

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.
2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.
3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.
4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.
(…)
12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.'

With regard to the matters governed by these provisions, account is taken of recitals 124, 125, 126 and 130 of the GDPR, in particular the following:

(124) '... that authority (the lead authority) should cooperate with the other authorities

concerned...'.
(125) 'as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process'.
(126) 'the decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned...'.
(130) 'Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority'.

In accordance with Article 4 (24) GDPR*, 'relevant and reasoned objection*' means the following:

'An objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union'.

In accordance with the above rules, in the present case, concerning a complaint lodged with the supervisory authority of a Member State (the Netherlands), in relation to processing operations in the context of the activities of an establishment of a controller which affect or are likely to substantially affect data subjects in more than one Member State (cross-border data processing), the lead supervisory authority, in this case the Spanish Data Protection Agency, is required to cooperate with the other authorities concerned.

The Spanish Data Protection Agency, in application of the powers conferred on it by the GDPR, is competent to adopt decisions designed to produce legal effects, whether the imposition of measures ensuring compliance with the rules or the imposition of administrative fines. However, it is obliged to closely involve and coordinate the supervisory authorities concerned in the decision-making process and to take their views into account to the greatest extent. It also provides that the binding decision to be taken is to be agreed jointly.

Article 60 GDPR regulates this cooperation between the lead supervisory authority and the other supervisory authorities concerned. Paragraph 3 of that article expressly provides that the lead supervisory authority shall, without delay, forward to the other supervisory authorities concerned a draft decision for its opinion and shall take due account of its views, in accordance with the procedure laid down in paragraphs 4 et seq. The supervisory authorities concerned have a period of four weeks to raise reasoned objections to the draft decision, it being understood that there is agreement on the draft decision if no authority objects within the period indicated, in which case all of them are bound by the repeated draft.

In another case, i.e. if any of the authorities concerned raises a relevant and reasoned objection to the draft decision, the lead supervisory authority may follow the objection by submitting to the opinion of the other supervisory authorities concerned a revised draft

decision, which shall be submitted to the procedure referred to in paragraph 4 within two weeks. If no further action is taken in the objection or if the objection is deemed not to be relevant, the lead supervisory authority should refer the matter to the consistency mechanism provided for in Article 63 GDPR.

In the present case, the AEPD initially considered that there were no indications of an infringement and, therefore, on 28 September 2020, a draft decision was issued, whereby the other supervisory authorities concerned were required to discontinue proceedings (Draft decision).

At the end of the prescribed period, the Data Protection Authority of the Netherlands (Autoriteit Persoonsgegevens -AP) objected to the draft decision in the sense set out in the background to this act.

Taking into account the reasons set out in the objections raised, and in accordance with Article 60(1) of the GDPR, as transcribed above, which obliges the lead supervisory authority to cooperate with the other authorities, in an effort to reach consensus, the procedure provided for in Article 60 (5) was followed instead of resorting to the consistency mechanism provided for in Article 63 of the GDPR.

Although this Agency initially considered that there were no indications of infringement, following an analysis of the observations or objections raised by the supervisory authority concerned, certain circumstances were revealed which had not been sufficiently assessed in the draft decision, which will be set out in the following legal grounds.

It was therefore appropriate to draw up a revised draft decision providing for the opening of penalty proceedings against MARINS PLAYA.

This is in line with the cooperation procedure regulated in Article 60 GDPR; it also takes into account Article 58 (4) of the same Regulation, according to which the exercise of the powers conferred on the supervisory authority must respect the procedural safeguards laid down in Union and Member State law.

Spanish procedural rules, in particular Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), provide that proceedings of a sanctioning nature shall always be initiated ex officio by agreement of the competent body, which must contain, among other information, the identification of the person or persons presumed to be responsible, the facts giving rise to the initiation of the proceedings, their possible classification and the penalties that may apply.

The adoption of this draft agreement to initiate penalty proceedings is provided for in Article 64 (2) (third subparagraph) and (3) of the LOPDGDD, with the obligation to give formal notice to the person concerned. That notification interrupts the limitation period for the infringement.

The revised draft decision drawn up by the AEPD, in the form of a draft decision to initiate penalty proceedings, was submitted for consideration by the authorities concerned, so that they could raise any objections they considered relevant or agree to it. To that end, it was sent via the IMI system to those authorities, informing them that, if no objections were raised within two weeks of the consultation, the necessary agreement to initiate

penalty proceedings would be adopted. The concerned supervisory authorities did not raise any objections and it was therefore understood that there was agreement on the draft in question.

Consequently, on 19 July 2021, the AEPD decided to initiate the present penalty proceedings, in accordance with the arguments and allegations contained in the revised draft decision.

Furthermore, Article 64 (4) of the Spanish LOPDGDD provides that the handling periods laid down in this Article are automatically suspended when information, consultation, request for assistance or mandatory pronouncement must be obtained from a body or agency of the European Union or from one or several supervisory authorities of the Member States in accordance with the GDPR, for the time between the request and the notification of the pronouncement to the Spanish Data Protection Agency.

III

Article 6 of the GDPR refers *to 'Lawfulness of processing*' in the following terms:

'1. Processing shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official
authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
(a) Union law; or
(b) Member State law to which the controller is subject.
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for

in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.
4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation'.

Account is taken of recitals 40 to 45 and 47 of the GDPR in relation to Articles 6 and 7 of the GDPR referred to above.

In the present case, a complaint is lodged against MARINS PLAYA for, during the process of registering the complainant in the hotel, a digital scanning of his passport, of the whole document, despite the opposition expressed by him; as well as the use of the personal data contained in that document, including the photograph, for the control and billing of the customer's consumption during his stay.

The steps taken have shown that the scanning process to which the customer's identification document is submitted on arrival at the hotel is not intended to obtain a digital image of the entire document. As detailed in Degree 2, the scanning is carried out using optical character recognition (OCR) software that automatically identifies the characters of a certain alphabet and stores them in data form, i.e. converts the image into text. This is a support programme that captures the customer's data, integrates it into the entity's information system and makes it possible to complete the *'customer file'* or *'passenger entry report'*.

There is no evidence that the entity has a complete picture of the customers' identity document. Nor does it appear that the scanned image of that document was incorporated into the devices used by hotel staff (bar and canteen).

If, on the other hand, it is established and acknowledged by MARINS PLAYA itself that, by means of that process, that entity collects the personal data of its customers concerning the number, type and date of issue of the identity document presented, name, sex, date and country of birth, as well as the photograph; these are referred to the State Security Forces and Corps in compliance with the rules on public safety and used for *'hotel management'*, in accordance with the terms used by the entity itself in its reply to the AEPD Inspection Services.

This includes the use of personal data by administrative and service staff. According to the documentation provided by the entity, service staff use a device that incorporates information on customers, including room and booking numbers, number of persons and departure date; name of the person, scheme, type of VIP and number of visits, as well

as the customer's photograph, which is checked to verify the identity of the customer when making consumption at the hotel; however, they do not have the scanned image of the identity card.

The data collected, other than the photograph, are necessary for the performance of the contract to which the data subject is a party and for compliance with a legal obligation applicable to the controller. Therefore, the processing of these data is covered by Article 6 (1) (b) and (c) GDPR.

The rules governing registers and reports of entry of travellers in hospitality establishments, as well as the obligation to communicate the information contained in hotels and registers to police offices, consist essentially of Organic Law 4/2015 of 30 March 1995 on the protection of public safety and Order INT/1922/2003, of 3 July, on registration lists and records of entry of passengers in hospitality and similar establishments.

Article 24 (1) of Spanish Organic Law 4/2015 provides:

'Natural or legal persons carrying out activities relevant to public safety, such as accommodation..., shall be subject to the obligations of recording documents and information in accordance with the terms laid down in the applicable provisions.'

This Organic Law, and the aforementioned Order detailing those obligations, legitimise the collection of personal data relating to identity card numbers, type of document and date of issue, name, sex, date of birth and country of nationality, date of entry and signature of the traveller; these must be added to the 'Record' that the entity responsible for the hotel must transfer to the State Security Forces.

It is therefore necessary to determine the scope to be given, from the point of view of the personal data protection, to the collection and use of photographs of customers carried out by MARINS PLAYA.

In that regard, the first point to be noted is that the information on the protection of personal data provided to customers by the entity did not include any details on the collection and use of the photograph and were therefore unknown to the data subjects. In fact, even the data processing to which the photograph is subjected does not appear in the Record of Processing Activities.

The arguments put forward by MARINS PLAYA in its written observations to the proposal for a resolution when it states that customers were informed during the registration process at the hotel establishment must therefore be rejected. It is true that, with this statement of arguments, it provided an information document which does refer to the registration of the photograph in the company's systems, but it has not proved that this document was delivered to customers, nor did it justify when it implemented its use.

In that regard, it should be noted that, at the stage of the evidence in the proceedings, the Agency expressly requested the organisation to copy its privacy policy, in all its versions in force from 25 May 2018 and of any privacy notice or additional information, as well as details of the channels authorised to disclose this information, and that organisation did not submit the information document which it now submits with its

arguments to the proposal for a resolution.

With regard to the customers' photographs, MARINS PLAYA has stated that the image is used to provide hotel staff with the identification of the customer who is using the credit or room card (at the time of consumption, the customer provides that card to the employee, who, on passing it to make the charge, can check the photograph), as well as to control access to the premises. When the customer registers, he/she is provided with a magnetic card allowing him/her, in addition to access to the room, to pay for consumption from his/her account, which he/she will pay at the end of his/her stay. At the time of consumption, the customer provides that card to the employee, who, by passing it through his/her device to make the charge, sees the customer's photograph.

The collection and use of customer photographs are not covered by the above-mentioned legal bases (performance of the contract and fulfilment of a legal obligation).

According to MARINS PLAYA, it is intended to verify the identity of the customer in order to prevent fraudulent use of the card by third parties and to prevent serious economic damage to the customer; no fees are paid with a lost card that is not the responsibility of the user of the service. On this basis, the aforementioned entity considers that this processing is covered by Article 6 (1) (f) of the GDPR, since there is a legitimate interest of the controller in charging the real user of the service and the customer, preventing the use of cards in a fraudulent manner and ensuring that the consumption made by third parties is debited from customers' accounts.

The existence of a legitimate interest of the responsible entity and of the customer itself is invoked as a legal basis covering the processing of customers' photography.

As regards the legal basis of the legitimate interest, Article 6 provides:

"1. Processing shall be lawful only if and to the extent that at least one of the following applies:
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child…'

Recital 47 of the GDPR specifies the content and scope of this legitimate basis for processing:

'The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The

processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.'

The interpretative criteria drawn from this recital are, inter alia, (i) that the legitimate interest of the controller overrides the interests or fundamental rights and freedoms of the data subject, in the light of the data subject's reasonable expectations, based on his or her relationship with the controller; (II) it is essential that a '*careful assessment*' of the rights and interests at stake be carried out, including in cases where the data subject can reasonably foresee, at the time and in the context of the collection of data, that processing for that purpose may take place; (III) the fundamental rights and interests of the personal data subject could prevail over the legitimate interests of the controller where the processing of the data is carried out in such circumstances where the data subject' '*does not reasonably expect'* that further processing of his or her personal data will take place.

MARINS PLAYA has not justified that legitimate interest sufficiently to allow the balancing of the interests of the controller against the rights of the data subject, which is necessary to determine the lawfulness of the processing carried out. In the present case, moreover, it does not appear that that entity carried out that balancing test and duly informed the complainant on that legitimate basis.

During the proceedings, the Agency expressly asked the entity to provide *'a copy of the documents containing the assessment of whether or not the interests and fundamental rights of the customers take precedence over the interests of MARINS PLAYA, in relation to the processing operations of customers' personal data carried out under the responsibility of MARINS PLAYA seeking to satisfy legitimate interests pursued by MARINS PLAYA itself or by a third party'.* This entity responded to the agreed request for evidence, but did not provide any documentation relating to the processing of personal data based on legitimate interest.

The entity did not carry out this preliminary analysis, even though it refers to it in its written submissions to the proposal for a resolution, and at no time does it inform customers on this legal basis of the processing. With regard to the information document submitted with that letter, which contains a reference to the legitimate interest, we refer to the above information letter.

In the absence of information concerning the balancing test, the data subject is deprived of his or her right to know the legal basis for the processing alleged by the controller, and in particular, by referring to the legitimate interest, is deprived of his/her right to know what those legitimate interests alleged by the controller or of a third party would justify the processing without his/her consent being taken into account.

Similarly, the data subject is deprived of his or her right to plead on what grounds that legitimate interest relied on by the controller could be counterbalanced by the rights or interests of the data subject. If the data subject was not given the opportunity to rely on them against the controller, any balancing carried out by the controller without taking into account the circumstances which might be invoked by the data subject who has not been allowed to do so would be vitiated by an act contrary to a mandatory rule.

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

when such processing is carried out in a hidden manner.

That legal basis for a legitimate interest cannot therefore be relied on in the context of an administrative procedure, such as the transfer of the complaint or the submission of arguments to the initiation of penalty proceedings. To accept this would be both to admit a legitimate interest arising, or a posteriori, in respect of which the requirements laid down in the legislation on the protection of personal data have not been complied with and of which the data subjects are not informed.

Although the legitimate interest is not applicable, it is important to analyse the terms in which the balancing of the legitimate interests of the data controller and the protection of personal data of the data subject, that is to say how that legitimate interest, if applicable, must be carried out in accordance with Article 6 (1) (f) of the GDPR.

The ECJ, in its judgment of 04 May 2017, C-13/16, Rigas Satskime, paragraphs 28 to 34, determined the conditions for a processing to be lawful on the basis of a legitimate interest. The ECJ judgment of 29 May 2019, C-40/17, Fashion ID, echoing the aforementioned judgment, sets out those requirements.

28. In that regard, Article 7(f) of Directive 95/46 (now Article 6 (1) (f) GDPR) lays *down three cumulative conditions for the processing of personal data to be lawful: first, the controller or the third party or parties to whom the data are disclosed pursue a legitimate interest; second, processing is necessary for the purposes of that legitimate interest and, third, the fundamental rights and freedoms of the data subject should not prevail.*

This legal basis requires the existence of real, non-speculative interests which, moreover, are legitimate. And not only the existence of such a legitimate interest means that the processing operations can be carried out. Such processing also needs to be necessary to meet that interest and to consider the impact on the data subject, the level of intrusion on his or her privacy and the effects that may have a negative impact on the data subject.

As regards the first of the conditions, namely that the controller or third parties pursue a legitimate interest, such as preventing the fraudulent use of the card which the requested person issues to its customers, we are faced with an interest which could be regarded as legitimate in itself, although that interest must be balanced against that of individuals. In other words, even if the controller has such a legitimate interest, that does not mean, in itself, that that legal basis can simply be relied on as a basis for the processing. The legitimacy of that interest is only a starting point, one of the factors to be weighed up.

As regards the second condition, however, it is considered that the processing of personal data carried out by MARINS PLAYA is not necessary or strictly necessary for the purposes of the legitimate interest alleged (Case C-13/16 Rigas Satskime, cited above, paragraph 30, '*As regards the requirement that the processing of data be necessary, it should be borne in mind that exceptions and restrictions to the principle of the protection of personal data must be established within the limits of what is strictly necessary*').

This principle, according to which processing must be strictly necessary for the purposes of the legitimate interest, must be interpreted in accordance with Article 5 (1) (c) GDPR, which refers to the principle of data minimisation, stating that personal data shall *be*

'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.

In this way, less intrusive means should always be preferred to serve the same purpose. Necessity here presupposes that processing is indispensable to the satisfaction of that interest, so that, if that objective can reasonably be achieved in another way which produces less or less intrusive impact, the legitimate interest cannot be invoked.

The term '*necessity*' used in Article 6 (1) (f) GDPR has, in the view of the ECJ, its own and independent meaning in Community law. This is an '*autonomous concept of Community law'* (judgment of the Court of Justice of 16 December 2008, Case C-524/2006, paragraph 52). On the other hand, the European Court of Human Rights (ECtHR) has also provided guidance on how to interpret the concept of necessity. In its judgment of 25 March 1983, it stated that, notwithstanding the fact that the processing of complainants' data is *'useful'*, *'desirable'* or *'reasonable'*, as the ECtHR stated in its judgment of 25 March 1983, the word *'necessary'* does not have the flexibility implied in those expressions.

The more *'negative'* or *'uncertain'* the impact of the processing may be, the more unlikely it is that the processing as a whole can be considered legitimate.

As can be seen, the foregoing is consistent with the case-law of the Spanish Constitutional Court on the proportionality test to be carried out on a measure restricting a fundamental right. According to that doctrine, three conditions must be met: appropriateness (if the measure achieves the proposed objective); necessity (no other more moderate measure); proportionality in the strict sense (more benefits or advantages than harm).

In short, apart from the fact that the data subject does not know for what purposes or for which legal basis his/her data have been collected, it is understood that the collection and use of the photograph of the clients that MARINS PLAYA carries out constitutes excessive processing of personal data.

In relation to this issue, all the arguments put forward by the Dutch Data Protection Authority, referred to in the Fourth Fact, are used to call into question the processing of such personal data under Article 6 (1) (f) of the GDPR, considering that there are other less intrusive ways to verify whether the holder of the magnetic card is the legitimate holder of the card at the time of payment and thus to prevent such cards from being used fraudulently.

Furthermore, it is also not apparent from the actions that MARINS PLAYA has established additional safeguards that could favour the acceptance of this legal basis for data processing, such as promoting the data subject's right to object or establishing opt-out mechanisms.

In short, the legitimate interest invoked by MARINS PLAYA does not outweigh the fundamental rights and freedoms of data subjects in the protection of their personal data, so that the processing of personal data which it carries out cannot be considered to be covered by the legitimate interest provided for in Article 6 (1) (f) GDPR.

Nor does the data subject give consent to such data processing. In accordance with the provisions referred to above, the processing of personal data which is the subject of the complaint requires the existence of a lawful legal basis, such as the consent of the data subject validly given, where there is no other legal basis referred to in Article 6 (1) GDPR or the processing pursues a purpose compatible with that for which the data were collected.

Article 4 of the GDPR *defines 'consent'* as follows:

"Article 4 Definitions
For the purposes of this Regulation:
(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'

In relation to the provision of consent, the provisions of Article 6 GDPR, cited above, and Articles 7 GDPR and 6 LOPDGDD should be taken into account.

Article *7 "conditions for consent*" of the GDPR:

'1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.'

Article *6 "processing based on the consent of the data subject*" of the LOPDGDD:

'1. In accordance with the provisions of article 4.11 of Regulation (EU) 2016/679, consent of the data subject shall be understood as any freely given, specific, informed and unambiguous indication through which they agree, by means of a declaration or a clear affirmative action, to the processing of personal data relating to them.
2. When it is intended to base the processing of data on the consent of the data subject for different purposes, it shall be necessary to state specifically and unequivocally that such consent is granted for all of them.
3. The performance of the contract may not be conditioned to the data subject authorising the processing of the data for purposes which are not related to the maintenance, development or control of the contractual relationship'.

Consent is understood as a clear affirmative act reflecting a freely given, specific, informed and unambiguous indication of the data subject's wishes to accept the processing of personal data concerning him or her, provided with sufficient safeguards

to demonstrate that the data subject is aware of the fact that and the extent to which he or she gives his or her consent. And should be given for all processing activities carried out for the same purpose (s), so that, where the processing has several purposes, consent should be given to all of them in a specific and unambiguous manner, without the performance of the contract being made conditional on the data subject's consent to the processing of his or her personal data for purposes other than the maintenance, development or control of the trading relationship. In this respect, the lawfulness of the processing requires that the data subject be informed of the purposes for which the data are intended (informed consent).

Consent must be given freely. It is understood that consent is not free when the data subject does not have a genuine or free choice or cannot refuse or withdraw consent without detriment; or where he/she is not allowed to authorise separately the different processing operations of personal data despite being appropriate in the specific case, or where the performance of a contract or service is dependent on consent, even if consent is not necessary for such performance. This is the case where consent is included as a non-negotiable part of the terms and conditions or when there is an obligation to agree to the use of personal data additional to what is strictly necessary.

Without these conditions, the provision of consent would not give the data subject genuine control over his/her personal data and the destination of the data, thereby rendering the processing activity unlawful.

The Article 29 Working Party analysed these issues in its *document "Guidelines on consent under Regulation 2016/679*", revised and approved on 10 April 2018; this has been updated by the European Data Protection Board on 04 May 2020 through the document *"Guidelines 05/2020 on consent under Regulation 2016/679"*. From what is stated in this document, it is now important to highlight some aspects related to the validity of the consent, in particular on the elements "specific", "informed" and "unambiguous":

'Article 6(1)(a) confirms that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them.28 The requirement
that consent must be 'specific' aims to ensure a degree of user control and transparency for the data subject. 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 requirement for 'granularity' to obtain 'free' consent.29 In sum, to comply with the element of 'specific' the controller must apply:
i Purpose specification as a safeguard against function creep,
ii Granularity in consent requests, and
iii Clear separation of information related to obtaining consent for data processing activities from information about other matters. 56.

Ad. (i): Pursuant to Article 5(1)(b) GDPR, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity.30 The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control. 57.

If the controller is relying on Article 6(1)(a), data subjects must always give consent for a specific processing purpose.31 In line with the concept of purpose limitation, Article 5(1)(b) and recital 32, consent may cover different operations, as long as these operations serve the same purpose. It goes without saying that specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.

Notwithstanding the provisions on compatibility of purposes, consent must be specific to the purpose. Data subjects will give their consent with the understanding that they are in control and their data will only be processed for those specified purposes. If a controller processes data based on consent and wishes to process the data for another purpose, too, that controller needs to seek additional consent for this other purpose unless there is another lawful basis, which better reflects the situation…
Ad. (ii): Consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'. This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes. 61.

Ad. (iii): Lastly, controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement that controllers must provide clear information, as discussed in paragraph 3.3. below'.

'3.3 Informed
The GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.
The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.'

'3.3.1 Minimum content requirements for consent to be 'informed'
For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, the EDPB is of the opinion that at least the following information is required for obtaining valid consent:
i. the controller's identity,
ii. the purpose of each of the processing operations for which consent is sought,
iii. what (type of) data will be collected and used,
iv. the existence of the right to withdraw consent,
v. information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) where relevant, and
vi. on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.'

In the present case, there is no evidence of valid consent from MARINS PLAYA customers covering the processing of personal data carried out by MARINS PLAYA with the photograph of those customers. This entity does not even report on this use of the photograph, nor has it established any mechanism for customers to consent to this use by means of a separate affirmative act for these specific processing operations, which are also not included in the Record of Processing Activities.

Consequently, in accordance with the evidence set out above, the aforementioned facts

constitute an infringement of Article 6 of the GDPR, which gives rise to the application of the corrective powers conferred on the Spanish Data Protection Agency by Article 58 of the GDPR.

As can be seen from the above, the conclusions drawn on the facts analysed go beyond MARINS PLAYA's specific action in relation to the collection and processing of the complainant's personal data and relate to the personal data management process put in place by this entity in general. Therefore, contrary to what was stated by this entity in its written pleadings to the proposal for a resolution, it is irrelevant whether or not the complainant objected to the handing over of his passport at the time of registration at the hotel.

It is also irrelevant that the photograph of the customers was displayed only by the service staff. What matters is the processing carried out, which involves recording the photograph in the requested person's information systems, and the circumstances in which it is carried out.

Finally, it should be noted that the evidence completed in the proceedings makes it possible to reject the assertion made by MARINS PLAYA in its written pleadings to the proposal for a resolution that the photograph should be retained only during the customer's stay in the hotel and subsequently removed. The complainant's own factsheet, which was requested by the Agency, proves that his photograph is currently still kept in the entity's information system.

IV

In the event of an infringement of the provisions of the GDPR, among the corrective powers available to the Spanish Data Protection Agency as the supervisory authority, Article 58 (2) of the GDPR provides for the following:

'2 each supervisory authority shall have all of the following corrective powers:
(...)
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;'
(...)
(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
(...)
(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;'

According to Article 83 (2) GDPR, the measure provided for in point (d) above is compatible with the penalty consisting of an administrative fine.

V

The facts set out above do not comply with Article 6 of the GDPR, which entails the commission of an infringement under Article 83 (5) (a) of the GDPR, which, under *the*

heading 'General conditions for the imposition of administrative fines', provides:

'5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9.'

In this regard, Article 71 of the LOPDGDD states *that 'The actions and behaviours referred to in sections 4, 5 and 6 of Regulation (EU) 2016/679, as well as those which are contrary to this organic law, shall constitute infringements'.*

For the purposes of the limitation period, Article 72 of the LOPDGDD states:

"Article 72. Infringements considered very serious.
'1. In accordance with article 83.5 of Regulation (EU) 2016/679, any infringement consisting on a substantial infringement of the provisions mentioned therein, especially the ones listed below, shall be considered very serious infringements and its limitation period shall be three years:
(...)
(b) The processing of personal data without any of the conditions for a lawful processing established in article 6 of Regulation (EU) 2016/679.'

In order to determine the administrative fine to be imposed, it is necessary to comply with the provisions of Articles 83.1 and 83.2 of the GDPR, which state**:**

'1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
(b) the intentional or negligent character of the infringement;
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor;
(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 manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.'

Article 76 of the LOPDGDD, entitled *'Penalties and corrective measures'*, provides:

'1. Penalties provided by sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679 shall apply considering their degree and the criteria established in section 2 of the aforementioned article.
2. Pursuant to the provisions of article 83.2.k) of Regulation (EU) 2016/679, the following criteria may also be considered:

(a) The ongoing nature of the relevant infringement.
(b) The existence of a link between the perpetrator's activities and their processing of personal data.
(c) Any profits obtained as a consequence of the relevant infringement.
(d) The possibility that the perpetrator's activities have induced them to commit the relevant infringement.
(e)The existence of a merger by acquisition subsequent to the infringement, which may not be attributed to the acquiring company.
(f) Whether the rights of minors have been affected.
(g) The existence of a Data Protection Officer, in those cases when their appointment is not compulsory'.
(h) Voluntary submission by the data processor or the data controller to alternative dispute resolution methods, in those cases in which disputes arise between the data processor or the data controller and any other stakeholder.'

In accordance with the above provisions, for the purpose of determining the amount of the penalty to be imposed in the present case, it is considered that the penalty should be graduated according to the following criteria:

The following criteria for graduation are considered to be aggravating factors:

. Article 83 (2) (a) GDPR: *"(a)* '*(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them'.*

. As regards the duration of the infringement, it is apparent from the proceedings that the collection of personal data carried out by the entity, including the collection of the customer's photograph, has taken place since at least 27 August 2018, the date of entry into the complainant's hotel, and is currently being maintained.
. Number of data subjects: the infringement concerns all the entity's customers.
. The nature of damage caused to the data subjects, which has increased the risk to their privacy.

. Article 83 (2) (b) GDPR: *"(b) the intentional or negligent character of the infringement"*.

It should be noted that the procedure for collecting personal data put in place by MARINS PLAYA entails, from the point of view of the data subjects who are the holders of the data collected, the loss of disposal and control over their data, since they do not even know that that collection of data includes the photograph appearing on the identity document provided by the customer on arrival at the hotel.

Those circumstances, in addition to those referred to in the previous paragraph,

show that MARINS PLAYA acted negligently. In this regard, account is taken of the ruling of the National High Court of 17 October 2007 (rec. 63/2006), which, on the assumption that these are entities whose activities involve continuous processing of customer data, states that *'... the Supreme Court has understood that there is a lack of prudence whenever a legal duty of care is disregarded, i.e. when the infringer does not act with the required diligence. In the assessment of the degree of diligence, particular consideration must be given to the professionalism or otherwise of the data subject, and there is no doubt that, in the present case, when the appellant's activity is of constant and abundant handling of personal data, emphasis must be placed on rigour and care to comply with the legal provisions in this regard'.*

It is a company that processes its customers' personal data on a systematic and continuous basis and must take utmost care in complying with its data protection obligations.

In addition, it is considered that it has been informed on several occasions, during the processing of the complaint, of the possible irregularity in its action and has not taken any action to rectify it.

. Article 83 (2) (d) GDPR: *"(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32."*

The entity does not have adequate procedures in place for the collection and processing of personal data, so that the infringement is not the result of an anomaly in the operation of those procedures but of a defect in the personal data management system designed by the controller.

. Article 83 (2) (g) GDPR: *'(g) the categories of personal data affected by the infringement'.*

While *'special categories of personal data'*, as defined in the GDPR in Article 9, have not been affected, this does not mean that the stolen data was not of a sensitive nature. The personal data affected by the processing (the photograph of customers) is of a particularly sensitive nature, in that it allows for the prompt identification of data subjects and increases the risks to their privacy, especially when it is recorded in conjunction with all the data contained in the holder's identity card, as is the case here.

. Article 76 (2) (a) of the LOPDGDD: *'(a) the ongoing nature of the relevant infringement'*.

The procedure for collecting and processing personal data put in place by the entity applies to all customers for at least the period indicated when referring to the duration of the infringement. This is a number of actions following the action designed by MARINS PLAYA, which infringe the same provision.

. Article 76 (2) (b) of the LOPDGDD: *'(b) The existence of a link between the perpetrator's activities and their processing of personal data'.*

The fact that the infringer's activity is closely linked to the processing of personal data, taking into account its activity in the hotel sector and its volume of activity (see Fifth Fact for some details).

. Article 83 (2) (k) GDPR: *'(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.'*

MARINS PLAYA's status as a medium-sized enterprise and turnover (some details are given in Fifteenth Fact).

The following circumstances are also considered to be mitigating:

. Article 83 (2) (k) GDPR: *'(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.'*

Although the collection of personal data relating to the customer's photograph and subsequent use of it is considered excessive, account is taken of the aim pursued by the entity, which is to prevent fraud in the consumption of services, and that no use other than this personal data has been proven.

In view of the factors set out above, the assessment of the fine for infringement of Article 6 of the GDPR is 30,000 EUR (thirty thousand euros).

It should be noted that MARINS PLAYA has not put forward any arguments regarding the graduation of the penalty in the letter submitted in response to the proposal for a resolution drawn up by the Agency.

VI

Infringements may result in the controller being required to *take appropriate measures to bring its action in line with the rules referred to in this act, in accordance with the aforementioned Article 58 (2) (d) GDPR, according to which each supervisory authority may 'order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period'.*

In this case, the entity should be required to stop collecting and processing the photograph of its customers within the period specified in the operative part. Otherwise, it must adapt the data protection information it provides to customers, in particular on the collection and use of the photograph and the legal basis on which the processing is based, by establishing mechanisms to prove that this information is accessed by the data subjects; and to carry out the necessary alignment of the processing operations referred to in this act with the requirements of Article 6 (1) GDPR, with the scope expressed in the previous legal bases.

It will also have to correct the effects of the infringement committed, leading to the removal of all photographs collected from customers in the circumstances that led to the

finding of the infringement sanctioned in this act.

It should be noted that failure to comply with this body's requests may be regarded as a serious administrative offence because it *'does not cooperate with the supervisory authority'* in response to the requests made, and such conduct may be assessed when administrative proceedings are initiated with a financial fine.

Therefore, in accordance with the applicable legislation and assessing the criteria for graduation of penalties established,
the Director of the Spanish Data Protection Agency DECIDES TO:

FIRST: Impose a fine of 30,000 EUR (thirty thousand euros) on MARINS PLAYA, S.A. (NIF A07158223) for an infringement of Article 6 of the GDPR, which is classified in Article 83 (5) (a) of the GDPR as very serious for the purposes of limitation period in Article 72 (1) (b) of the Spanish LOPDGDD.

SECOND: To require MARINS PLAYA, S.A. to take the necessary measures within one month to bring its action into line with the legislation on the protection of personal data, with the scope set out in Legal Ground VI. Within that period, the entity must justify this request from the Spanish Data Protection Agency.

THIRD: Notify this resolution to MARINS PLAYA, S.A.

FOURTH: Warn the entity to pay the penalty imposed once this decision is enforceable, in accordance with Article 98.1 (b) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations ('the LPACAP'), within the voluntary payment period laid down in Article 68 of the General Collection Regulation, approved by Royal Decree 939/2005 of 29 July, in conjunction with Article 62 of Law 58/2003, on 17 December, by entering the tax identification number of the sanctioned person and the procedure number shown in the heading of this document, in restricted account No ES93 ***2100 8981 6302 0001 1719,***opened in the name of the Spanish Data Protection Agency at the bank CAIXABANK, S.A. If this is not the case, they will be recovered during the enforcement period.

Upon receipt of the notification and once enforceable, if the date of enforceability is between 1 and 15 days of each month inclusive, the time limit for voluntary payment shall be until the 20th day of the following month or immediately thereafter, and if it is between the 16th and the last of each month inclusive, the time limit for payment shall be until the 5th of the second month following or immediately following.

In accordance with Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

In accordance with Article 48.6 of the LOPDGDD, and in accordance with Article 123 of the LPACAP, interested parties may, by way of option, lodge an appeal against this decision with the Director of the Spanish Data Protection Agency within one month of the day following notification of this decision or direct administrative appeal to the Administrative Appeals Chamber of the National High Court. in accordance with Article 25 and paragraph 5 of the Fourth Additional Provision of Law 29/1998 of 13 July

on Administrative Jurisdiction, within two months of the day following notification of this act, as provided for in Article 46 (1) of that Law.

Finally, we would point out that, in accordance with Article 90.3 (a) of the LPACAP, the final administrative decision may be suspended as a precautionary measure if the interested party indicates it intention to lodge an administrative appeal. If this is the case, the interested party must formally inform the Spanish Data Protection Agency of this fact by submitting it via the Agency's electronic register [https://sedeagpd.gob.es/sede-electronica-web/] or through one of the other registers provided for in Article 16.4 of Law 39/2015 of 1 October. It shall also forward to the Agency the documentation proving that the administrative appeal has actually been lodged. If the Agency is not aware of the lodging of the administrative appeal within two months of the day following notification of this decision, it shall terminate the provisional suspension.

938-231221

Mar España Martí
Director of the Spanish Data Protection Agency