 File No.: EXP202100603

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. British citizen residing in Spain (hereinafter, the

claimant) dated 06/21/2021, filed a claim in English, before the Agency

Spanish Data Protection. The claim is directed against GSMA LTD. with

NIF N4004237F (hereinafter, the one claimed). The reasons on which the claim is based

are the following:

She was invited as a speaker in the edition of the MOBILE WORLD CONGRESS, (MWC)

June 2021, held in Barcelona. To this end, the option was given to register

for the event in "virtual", or "in person". For the "in-person" option, "the

claimed requests to upload special category data-passport details,

including photographs that are transferred to a processor located in a third country-,

for facial recognition for security purposes".

It states that the privacy policy (https://www.mwcbarcelona.com/legal/privacy-

policy), "establishes that the basis of treatment is consent, however, in

email has been declared to be based on article 6.1 c) of the GDPR, it is

that is, compliance with a legal obligation, referring to article 22.2 of

the LOPD and article 11.1.h of Organic Law 2/1986. not possible to register

as a face-to-face speaker without uploading (uploading) biometric data. despite trying

troubleshoot the issue to find an alternative, it has been necessary to upload my

passport for registration."

It considers that there is no valid legal obligation for this type of treatment of

face recognition.

On the other hand, neither the privacy policies nor the communications maintained with the

claimed through email, provide clear information on the

data transfers to a data processor in a third country.

While the policies do not refer to any sub-processor,

nor are transfers to third parties recognized, if it is done in documents referenced to

through

the privacy policy in a FAQ section,

https://www.mwcbarcelona.com/attend/event-entry/breez/breez-faq, which indicates

that:

"If you decide to participate in BREEZ (acronym for Biometric Recognition Easy Entry

Zone, easy access zone with biometric recognition), your biometric data will be

communicated to the following third-party provider that carries out the recovery activities:

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

facial knowledge of the Event: ScanVis Ltd.", considering the claimant who is

producing a transfer.

In communications with the GSMA, they have stated in an email: "Regarding

tion with your fourth point, the servers that process ID-related data are

located in Europe. There is no transfer of personal data to Russia. Our supplier-

chosen service provider has a global presence, despite being based in Bien-

lorussia. Please be assured that the GSMA only contracts with companies to

act on their behalf if such companies are able to provide representation

nes and guarantees against unauthorized transfer to third parties.”

“Although we have asked the GSMA for any standard contractual clauses or rules

relevant binding corporate laws, none have been provided.

“With reference to the recommendations of the European Committee for Data Protection

(CEPD) on measures that complement the transfer tools for

ensure compliance with the EU level of Personal Data Protection,

adopted on November 10, 2020, I believe that the GSMA has not considered the risk

potential transfer to a third country through remote access. Therefore, the

supposed confidence in the adequacy as an instrument of legal transfer is not

effective."

Provide a copy of the email chain exchanged from 05/20 to

06/4/2021, which are summarized:

Claimed, 05/20/2021, 10:16 a.m. Associated with an “invitation to register”. You

informs that MWC 21 is now contactless, for faster and safer access, with

mandatory pre-arrival identity verification for all attendees.

To enter MWC 21 and other events associated with the invitation. associate listed

the terms and conditions indicating that admission is subject to them. Links appear

for: “How to register”. Once you have filled in the complete “registration system”,

"You will receive an email confirmation with more information." "Please keep in mind:

There are no registration support areas at the MWC 21 venue, so make sure that

is fully registered before your arrival at the venue. Any error in it may

delay your access to the event”.

 Complainant, 05/20/2021, 10:39 a.m. “I would like to convey my concern about

your mandatory request, which was optional last year, about uploading/downloading my

documentation on its website” ”The passport or identity card is information

very private and share it with a third party that is not part of a structure

government, nor is it something I am required to do by law" "does not provide

information about how this information will be stored, shared".

 Claimed, 05/20/2021, 11:41 a.m. Please note that this year you are required to

"upload" your ID. We do this identity verification in the

registration, since paper credentials or "on-site" registration will not be provided

(in the place).

"Using facial recognition technology, attendees can have a

Instant identity verification when they register using the option

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/48

BREEZ. We will take your passport image and use biometric tokens to

Match this against the photo we will take of you during the registration procedure.

tro. All persons entering Spain must be fully registered to

the MWC 21. He states that they work together with the Mossos d' Esquadra in the security plan

security to identify and redirect potential security threats. picking up the

identification of attendees is one of the means to improve our security

general and that of the assistants. Indicates two address links, one from the privacy policy

vacancy and another of the terms and conditions of assistance to expand that information.

tion.

Complainant, 05/20/2021, at 11:19 a.m., who insists that his issues have not

been answered.

Claimed, 05/28/2021, at 10:46 a.m. Indicates that information is available

about the process required for identification, the recipients and the period of retention on a registration faqs page, and on the privacy policy page, as well as in the registration process. “In summary, the GSMA organizes the MWC together with the Spanish authorities. Passport and identification details are required by the Spanish police, Mossos d' Esquadra. Please note that this is not a new requirement. However, the manner in which this information is provided, electronically, has changed for 2021, because businesses need to have a non-contact environment.” That being said, keep in mind that identification, data of identification and the fact of providing the passport, it is not obligatory for the virtual pass holders, who may attend without providing such information.”

 Complainant, 05/28/2021, 11:26 a.m. It indicates that the website suggests that the person can select, not opt-out, by automatic registration, "and it is something that like to do". It also alludes to the fact that the website mentions health reasons for uploading the documentation, but this would not justify uploading the passport and the photo for not keeping relationship, and that on the web it can be deduced that the data is transferred to an entity Belarus, with the dangers that this entails.

 Claimed, 06/2/2021, 2:53 p.m. He explains that MWC 21 offers options, in person and virtual. The virtual does not require you to upload an identification document. If you choose to attend in person, then identity verification is required. given by the Mossos d` Esquadra, a Spanish police force that does not make exceptions for residents in Spain. All attendees must have their identity verified.”

“the measure is not related to COVID…”” In the previous Congresses all attendees had to carry their identification on a credential card. The ninth-The reality for this 2021 is that this verification will be done digitally before the event,

due to non-contact environment. For identity verification in digital, to all

users are required to upload an image of their identity document and

provide a photograph of themselves. Attendees have two options:

-“ an automatic verification that uses facial recognition technology to match

Check the image of the identity document with your photo. These assistants can use

own queues for facial recognition to access the event”.

-A manual verification that is carried out by an agent who visually compares

the two images. These attendees can access the venue by scanning their code

QR on your digital badge which contains your photo. This process does not use any tech-

facial recognition technology.

"You must select the second option if you do not want automatic verification."

"In relation to your fourth point, the servers that process the identification data

are established in Europe. There is no transfer of personal data to

Russia. Our selected service providers have a global presence

despite the fact that its headquarters are in Belarus. GSMA only contracts with companies that

act on their behalf if such companies are able to provide warranties

aunts against transfers to third parties.”

 Complainant, 06/2/2021, 4:18 p.m. “I don't want to be a virtual speaker. But not

I'm sure I understood how to register without uploading my passport. not me

It doesn't matter if I get verified at the counter, but I don't want my data to be

stored anywhere. How do I proceed? He adds that the local authorities

they can access data from companies, to servers operating in Belarus.

 Complainant, 06/3/2021 at 11:10 a.m. "I still haven't received your response about

how to proceed with the registration in the real event without downloading my documents”

The deadline for registration is June 6. Please note that the reasons for

security displayed on your website is not a valid legal basis of article 6 of the GDPR.

Request, send you:

-Copy of the standard contractual clauses with the company in Belarus

-The accreditation that has carried out an impact evaluation of the transfers-

references to determine whether the laws of Belarus are adequate.

-Specify what technical measures have been implemented to prevent access to

I am from the Belarusian authorities.

 Claimed, 06/04/, 2:59 p.m. It tells you that the processing of your data takes place

in Europe and that use standard contractual clauses, or adequacy decision

from third countries and other legal tools to transmit the data outside the

European Economic Area or Switzerland. "While the treatment of the data of

identification is relevant to achieving security objectives, requirements

established by article 22.2 LOPD and article 11.1h) for the application of the

Organic Law 2/1986, GSMA treats the data as requested by the Mossos d`Esquadra,

in application of article 6.1.c) of the GDPR."

 Complainant, 06/4/2021, 5:42 p.m. “requesting that you explain what you mean, in

as soon as any personal data from the EEA and/or Switzerland is transferred to a third country

outside the EEA or Switzerland, unless it is an adequacy country as defined by the Co-

mission, standard clauses or other legal transfer tool is executed

gives."

If my passport is not a passport of the countries of the European Economic Area and

Switzerland, does this mean that my personal data will be transferred outside of the EEA? if this

is the case, I would like to know to which country and see the standard contractual clauses. It's a

GDPR right to request it.”

SECOND: For being related and being mentioned either in the claim, or in the

emails, they are reviewed;

a) Clause of "general terms and conditions for assistance" MWC

2021, Barcelona" in which attendees have to accept these conditions,

including, among others, registering for an account on the website, registering

in the event through the website, accept an invitation to an event.

It states: “Identification: You agree to carry a photo identification issued

by your government in the form of a passport or national identification card of the

UE with you at all times during the Event. You will be asked to submit di-

cha id. You are solely responsible for the accuracy of all data.

Personal data provided when registering for the Event…”

b)

“privacy policy”, last update 04/29/2021.

In: “When does the privacy policy apply?

ad ”, applies to various groups

participants in the MWC, among other speakers or speakers, assistants, in

relation to the personal data obtained, via: the attendance registration system

event app, digital and/or printed credential cards, or the system

facial recognition scanning mama (at access points, for session-

nes or to participate in closed-space meetings).

"Information you voluntarily provide."

"Account creation and registration": indicates various ways of collecting data with

examples “when you… create an account with us, you sign up for the

event, ...you require a service…””The information collected includes, but is not limited to,

limit to: your name, position, company name, work address, work email

under, job functions, phone number, area of interest, and photo. Yeah

you are a speaker, as additional information, your professional profile

“Automatic identity validation (facial recognition, RF)”. with his

consent, if you choose to register at MWC Barcelona through “validation

of automatic identity”, we can process your biometric data (through the use

of RF technology) during the online registration process and when you attend the

event, strictly for the limited purposes of verifying your identity. If you use

this process during registration, RF technology matches

automatically the image you provide us with the photograph on your

Passport/EU National Identity Card. This RF technology analyzes

their facial features by taking measurements of the data points that make up the

expensive. These data points include the distance between your eyes and the distance

from in front of the chin, etc. The technology processes a series of data points

data to create a map of your face in real time. This becomes a

secure data pattern using a complex algorithm to create your token

biometric (biometric file, identifier). For access security purposes

to the enclosure, we will automatically match the image taken at the point of

access against your biometric token token (ie your facial map). How I know

explained in the section: “your choices and control selection”, below, you can

withdraw your consent to the use of your biometric data in any

moment. If you do, we will remove your biometric token and the

manual validation of identity, as necessary (although removal of the

consent will not affect the legality of the processing of your biometric data

that has already taken place at the registration stage). Click here to get

more information about how we use facial recognition technologies

for identity verification purposes.

Typing in this space, leads to “BREEZ FAQS -FR (Easy entry zone

with biometric recognition--Frequently Asked Questions”. “The convenient way

registration in MWC”” is based on RF technology to provide

Create an ID via photo matching at registration in the

online registrations and identify and verify attendees from lists. Presents itself

as “RF technology to “Provide instant identity verification”

online through photo matching in the online registration system, and

Identify and verify registered attendees to allow access to facilities

event information and restricted areas (access to the BREEZ venue).

Free lanes are currently available at periphery access points.

the event and in the perimeter of the ministerial program.”

Who can use BREEZ?

All attendees can use BREEZ to speed up their identity check

in the automatic identity identification registration system, in addition to

take advantage of faster and smoother access control functionality during

the days of the event through BREEZ Venue access. Registration in BREEZ

it is completely voluntary.”

How can I sign up to use BREEZ?

“You can sign up for BREEZ during the event registration process or at

any time after you have registered for the event Follow these

easy steps:

1 “Give your explicit consent to use BREEZ

2 “By giving your consent, you will be prompted to have your photo taken through the system

ScanVis facial recognition theme for creating your biometric profile”.

3 “The uploaded photo will go through a quality check to ensure

that is suitable for facial recognition. If the parameters are met

defined, your biometric profile will be created. If not, you will be prompted to complete

the previous step again.”

4. “Your BREEZ photo will then be compared to your passport photo do-

European Union national identity card using your biometric profile.

co and a match score will be produced. If the score is below

above the threshold of the system, your identity will be confirmed, if not, your photos will be re-

endorsed and compared by a human being. This is the automatic validation of

ID”.

5. Once your registration is complete (payment / code provided), you will be

will enroll in BREEZ and will benefit from access to the BREEZ site, using the

BREEZ lanes on site, for a contactless experience.

A summary drawing with icons titled "automatic validation of

identity, what is automatic identity validation “we will use technology of

C / Jorge Juan, 6

28001 – Madrid

RF to automatically match the image we captured against the photo-

spelling in your passport national identity card. To do that we will create

a biometric token which will contain the sensitive information of the data on

their unique facial features."

It comes in a series of drawings, in the first one "does not wait": "The validation of the

identity will be completely instantaneous. Withdrawal of your consent

to use your biometric data for access to the facility, it will not affect the

processing of biometric data that has already been carried out for purposes

identity validation.

In the second drawing it says "safe and protected": "We take care of your data assuring

telling us that they are kept safe. For more information on how GSMA

will process your biometric data, to whom it may be disclosed and how to withdraw your

consent to the use of this biometric data for the MWC, please

see our privacy notice."

Finally, the last drawing: "easy access": "For access to the facilities, the

contactless use of BREEZ in queues will verify your image captured by the

cameras against your biometric token for identification validation purposes

tion. "

It is also stated at the bottom that "You consent to GSMA using

your biometric data obtained from the photographs provided by you

for identification validation purposes in the context of online registration

and for the MWC Barcelona for purposes of access to the venue", preceded by

a box that indicates "Yes, I consent to the use of my biometric data for validation

automatic giving of identity”.

How can I opt out of BREEZ?”

Your consent to participate in BREEZ remains valid as long as you maintain

have your MWC account or until you stop participating in BREEZ.

You can unsubscribe from BREEZ by withdrawing your consent at any time.

ment by accessing your registration account through https://register.mwcbarce-

lona.com/login and clicking the Unenroll button on BREEZ, or

contacting registration@mwcbarcelona.com.

If you do not consent to the use of BREEZ during the registration process,

has the alternative option of common/standard manual ID validation (management

via our Contact Center) at the time of registration and the

use of a digital badge (available in the My MWC events app

app) to access the venue. Your ability to attend the Event is not affected.

by a refusal/withdrawal of consent.

If you withdraw your consent before or during the Event, you will need to use your Badge

digital (available in the My MWC event app) and scan it each time

to enter the event. As discussed above, in addition to providing

BREEZ Venue Access, BREEZ provides Automatic ID Validation

ethics during the registration process by comparing the image of your passport /

EU national ID with your BREEZ profile to verify that the document

item entered matches the individual registrant. Please note that the

Automatic ID validation uses biometric data and occurs instantly

during the BREEZ registration process. The biometric token created for the

image matching process will be removed four (4) weeks after

of the end of the Event. Therefore, while you can withdraw your consent

of BREEZ at any time, there is no opportunity to withdraw consent.

Automatic ID Validation after that step of the process is completed.

registration cease.

Please note that although your consent remains valid as long as

maintain your MWC account, your biometric data is only retained for

4 weeks after the Event. This is an important step to protect your information.

training. Only when you register for a Later Event with your account at the

MWC, the biometric token will be regenerated.

How is my biometric data used and stored?

“After consenting to BREEZ and uploading a photo, our so-

facial recognition software analyzes facial features by taking measurements

measurements of the data points that make up the face. These data points

include the distance between your eyes and the distance from the forehead to the chin,

etc The technology processes a series of data points to create a map in

real time of your face. This is converted to a safe data pattern using

a complex algorithm to create your biometric token.

Your “biometric token” will be stored and retained in the European Union during the

duration of the Event and will be securely destroyed within 4 weeks

after the Event. GSMA is committed to protecting your personal data.

We have implemented appropriate technical and organizational measures to guarantee

ensure that your data is safe at all times. Each biometric token is encrypted

cold and stored in a separate database from the raw data used

two at its creation.

During the registration process, BREEZ is used to compare the image of your

passport/EU national ID card with your BREEZ profile for

complete Automatic Identity Validation. In the Event, BREEZ is used-

will be used to identify registered attendees to provide access to

BREEZ Venue. When you enter the BREEZ lane and approach a camera, be-

You will be recognized and granted access to the Event. This is done by matching

dir the real-time image of your face with the biometric token created during

the registration process."

To whom are my biometric data disclosed?

"If you choose to participate in BREEZ, your biometric data will be disclosed to the following

third-party provider that performs facial recognition activities for

the Event: ScanVis Ltd."

If BREEZ has no contact, can I leave my digital badge and ID

at the hotel?"

All attendees must have their digital credential available to enter the

external perimeter of the place. The digital credential will also be the only way to

access partner conferences or sessions.

Everyone in Spain is legally required to carry identification or pa-

Valid passport at all times. Therefore, attendees should keep di-

many identification documents with them during the Event."

THE PRIVACY POLICY SECTION CONTINUES:

Card/badge scanning

“We, or authorized third parties participating in the Event (including exhibitors)

sponsors and sponsors), we may collect your personal data by scanning your cre-

digital dental. This can occur when you access or leave the site, enter sessions

or other restricted areas at the Event, or enters an enclosed space, meeting room,

nions or restaurant. This scanning can occur for access control purposes, analysed.

lysis, event planning, logistics, health and safety (including prevention of

disease spread and contract tracking purposes) and to share

with a third-party session provider if you have scanned your digital badge or registered

to attend the session of that third party.

“,

" Share information

“We do not sell personal information to anyone and we do not disclose your data

personal data to third parties for independent use, unless": (highlighting

just a few points)

“You have consented that your biometric data obtained through information technology

facial recognition during registrations for access and to the venue are accessible

by third parties-click here for more information on who these third parties are

parts”.

“It is provided to any competent body in charge of enforcing the

law, regulator, government agency, court or other third party, to enforce a

agreement we have with you or to protect our rights, property or

safety, or the rights, property, or safety of our employees or

others. This includes law enforcement agencies

for security purposes and the health authorities, as appropriate.

necessary to prevent the spread of disease, including Covid-19 (for

example, for contact tracing purposes or to facilitate entry into Spain).

“Legal basis for the processing of personal information”

“…we will normally collect your personal information only when we have your con-

feeling to do so, when we need the personal information to perform a

contract with you, or when the processing is in our legitimate interest and is not annulled

side for their interests in Data Protection or fundamental rights and freedoms.

In some cases, we may also have a legal obligation to collect your information.

how can we be asked to do so for reasons of public interest?

or that we need the personal information to protect your vital interests or the

of another person, for example in case of a medical emergency during the event. Yeah

We ask you to provide personal information to comply with a legal requirement.

gal or to perform a contract with you, we will make this clear and inform you if the

provision of your personal information is mandatory or not (as well as the possible consequences

consequences if you do not provide your personal information. We are legally obligated

two to provide the personal data of the attendees and the provider's staff,

that is, name, date of birth, nationality, type of document number and date of

date of issue, to law enforcement authorities in connection with

event security. Any failure to provide this information will mean

that we cannot without registering you for the event and/or allowing you access to the venue.”

“Transfer of your information to the European Economic Area EEA, United Kingdom and

Swiss."

It informs that GSMA Ltd is based in the USA. “By using your information as is-

set out in this privacy policy, may be transferred to countries outside of the EEA, the

UK and Switzerland. By way of example, this can also happen if one of our

After partner companies or our service providers are in a

country outside the EEA, the UK or Switzerland. When we transfer personal data

from the EEA, UK and Switzerland to other countries, we use a variety of me-

legal mechanisms, including the standard contractual clauses adopted by the Co-

EU mission to ensure your rights and protections travel with your data.

"Data retention"

[…]”

“When you have consented to automatic identity validation, delete

we will mine your biometric token (your facial map) within 28 days after the

last day of the event.

“Your choices and control”

[…]”

“Similarly, if we have collected and processed your personal information about the

based on your consent, you can withdraw it at any time.

“When we process your personal data automatically, for example when we carry-

we carry out automatic identity validation, you have the right to challenge a decision

decision to deny you entry to the event based solely on this self-validation.

identity to the extent that such a decision has a legal basis

or a similar significant effect on you. In such circumstances, you have the right to ex-

express your point of view and request a human review of the decision. can exercise

this right by contacting the contact center prior to the event, at which

In this case, it may be necessary to manually validate the identification and/or carry out other checks.

appropriate security controls.

The last section, "contact us", indicates: "If at any time you want to contact

with us with your views on our privacy practices or any

other query regarding your personal information, or if you do not want us to continue

using your information as indicated above, you can request it by email to

dataprivacy

@gsma.com

or write to Data Privacy-Legal, GSMA Ltd. The Walbrook

Building 25 Walbrook, London."

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

THIRD: In accordance with article 65.4 of Organic Law 3/2018, of 5/12,

Protection of Personal Data and guarantee of digital rights (hereinafter

LOPDGDD), said claim was transferred to the claimed party, -headquarters of

London – E/8199/2021, so that it "proceeds with its analysis and informs this Agency

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

sites provided for in the data protection regulations, and specifically:

1. The decision adopted regarding this claim.

2.

3.

Report on the causes that have motivated the incidence that has originated the claim

mation.

Report, if applicable, on the measures adopted to adapt its "Privacy Policy"

vacancy" to article 13 of Regulation (EU) 2016/679 of the European Parliament and

of the Council of April 27, 2016 (GDPR), implementation dates and controls

carried out to verify its effectiveness.

4. Justification of the legal basis on which the processing of biomedical data is based.

tricos, a circumstance that lifts the prohibition to deal with special categories of

data, according to article 9 of the GDPR, as well as the need to provide a copy

of the identification document for the accreditation of those attending the event.

5. The purpose of the treatment.

6. The information provided to the interested parties on the processing of their biological data.

metrics and, where appropriate, to obtain your consent.

7. Reasons justifying the necessity and proportionality of the use of bio-data

metrics for the purpose pursued.

8. Measures taken to ensure that data reuse is not possible

biometrics for another purpose.

9. Security measures adopted to protect the confidentiality of the data

personal

10. The Impact Assessment carried out or reasons why it has not been carried out (for

know the list of personal data processing that requires an evaluation

of impact, as well as any other information related to the evaluations

of impact, you can consult the "Manage EIPD" tool at https://www.ae-

pd.es/es/guias-y-herramientas/herramientas/gestiona-eipd)

11. Report on whether international transfers are made and, if applicable, whether there is

adequacy decision or adequate guarantees regarding inter-transfers

national data.

12. Supporting documentation on the relationship between the person in charge and the person in charge

of activities related to facial recognition.

13. Report on the measures adopted to avoid incidents occurring if-

thousands, dates of implementation and controls carried out to verify its effectiveness.

Inc.

14. Postal address of your representative in the European Union.

15. Any other that you consider relevant.

On 09/10/2021, this Agency received a written response that bears the

indication GSMA Ltd., at an address in Atlanta, USA. It begins by stating:

I am writing on behalf of GSMA Ltd. (GSMA) in connection with the letter sent

E/8199/21…".

According to information from the internet, GSMA (Global System for Mobile Communications,

"Global System for Mobile Communications") is an industry organization

of the mobile that brings together operators from all over the world, more than 750 operators of

mobile telephony and more than 400 Companies are associated as members. In the web

www.mwcbarcelona.com/legal which contains information on the Congress of

Barcelona 2022, it is indicated that "GSMA LTD with its main place of business

located in Atlanta, USA, a wholly owned subsidiary of the GSM Association, and

with respect to 4yfn 2022, GSMA 4fyn EVENT MANAGEMENT S.L., a subsidiary

of GSMA LTD., welcomes you to MWC BARCELONA 2022.", and that "GSMA LTD

and its affiliates provide you with the event…"

In response, state:

1) The claimant and the respondent continued in contact after the last copy

of mail of 06/04/2021 and a satisfactory resolution was achieved "registered for the

Congress as a virtual assistant and took part as a speaker in a round table", and

the respondent provided you with a "free virtual pass" and you were not required to download or upload

an identity document that was the element on which his claim was based. No

It is therefore true that the defendant "uploaded the passport."

2) Provides, for clarification purposes, the statements contained in the

claim and the correction estimated by the defendant, possibly due to

"possible misunderstandings."

a) Regarding whether the event is in person or virtual, the GSMA requires uploading or uploading data

such as the passport, which are transferred to a person in charge in a third country, manifests

that:

-An identification control was necessary for all face-to-face attendance at the

conference. Identity validation by FR (facial recognition) was optional.

Identity verification was not required for most virtual passes.

"There was an option for identity validation to take place without the use of

of RF". "The FR solution was only one of the three options for the validation of

identity made available. Options include:

validation of identification with FR,

manual validation of identification sent online, (standard ID validation-

□

□

common identity validation).

and in limited circumstances, validation of identification on paper, face-to-face,

in situ.

He therefore considers that it is not entirely true that: "it is not possible to register as a face-to-face speaker without uploading biometric data". Only the option of identification with FR included the treatment of data of special categories, for which the explicit consent.

b) On the disagreement in the legitimizing basis of the treatment that derives from the privacy policy clause, states that not all forms of verification of identification required the use of FR technologies and that consent explicit is the legal basis on which the FR data have been processed, not having discrepancies in the information provided by the defendant, in terms of whether indicates that the basis of the treatment in the email that the claimant says having received article 6.1 letter c) of the GDPR was indicated, since, "separately, GSMA was required by law to provide certain information to the Mossos- name surname nationality, date of birth, identity document provided, date of issue and document number."

c) Information on data transfers and treatment managers will not be contained in the privacy policy. It was decided to provide that information to through a page of frequently asked questions, FAQ, so that it was easily accessible, thus appearing at https://mwcbarcelona.com/attend/event-entry/breez/breez-faq where service providers are also contained.

Regarding the statement of the defendant that "this establishes that the opt-outs are available, however, after correspondence by email, this is incorrect. An opt-out is only available for virtual assistance."

He states that in "frequently asked questions" they refer to the right to withdraw the consent in the "How do I unsubscribe from BREEZ" section. "The interested parses this option in the context of the registry (but is not related to the options available at registration stage). In addition, for registration purposes, it is incorrect to say that, except for "virtual" assistance, registrants will be required to send to the RF a copy of the identification. required a copy of identification in all cases except (most) passport passes

attendance

virtual, but FR was optional and registrants were invited to consent expressly for the processing of your biometric data. Applicants for registry could opt for standard identity validation instead of FR, which does not it affects your ability to register for the conference. Similarly, don't we received complaints that opting for a standard ID validation instead from FR will adversely affect the conference experience." "To MWC 2021,

approximately 20,000 delegates attended and our registration team received very few inquiries regarding identity verification processes, the most of which were of a technical nature.

3) It states that its privacy policy was updated for the MWC 2021, being its latest version, 04/29/2021.

4) "FR questions: FR technologies were used (when the person opted for this option and gave their express consent) to verify the identity of the delegates in

the event, for security purposes. This happened in both cases:

-When the person registers online, that is, FR is used to compare a photo

of the person taken at the time of registration with the photo of the identity document

who climbs up them, and,

-To allow access to the event facilities, (i.e. the token was verified

biometric on the pass of the delegates) automatically against their image using

FR technologies).

As explained above, delegates were able to choose verification of

common identification, which did not imply the use of FR technologies. Instead, the

people had the option of uploading a copy of their identity document and a

photo (taken at the time they registered) which were later reviewed

manually by a third party engaged by the GSMA for these purposes. Your access

was facilitated by security personnel reviewing the image stored on your pass

of conference in front of his aspect/appearance

In a small number of cases, manual identification checks on

person (i.e. checking the paper version of the identification documents)

also took place at the event venue (although exceptionally for

minimize the spread of covid-19, as detailed below) and only

made for certain types of passes.

Identity verification was not performed for the majority of delegates

who attended the event virtually.

As described above, only FR was required as one of the three options

available to register in person for the event.

As also noted above, the GSMA shared some of the information

obtained in the context of identity verification (excluding information

biometric when it is collected) with the Mossos, since it is legally required to

in accordance with article 11.1.h of Organic Law 2/1986, on Public Order. By

for security purposes, and to ensure that you have captured reliable information from the

identity document, the GSMA required the provision of a copy of the identity document

identity.

At MWC 2019, the GSMA allowed paper copies of the documents of

Identification will be manually verified when accessing the MWC headquarters. However

This option has been suppressed - with some exceptions - for health and safety reasons for the

2021 event, in order to minimize the risk of spreading COVID-19,

reducing queues and crowds at access points. This is in line

with the "action plan for congresses of the Generalitat of Catalonia" to which it is subject

to the GSMA and which expressly requires the replacement of manual processes by

digital processes Provide the link of this plan, dated 07/22/2020. Contains guidelines and

recommendations for the reduction of contagion by coronavirus for meetings and

congresses, which applies to organizers of conferences, congresses or

conventions, responsible for the implementation and coordination of measures between the

which include the preparation of a contingency plan to reduce the risks of

COVID-19.

In point 4.2.3.2 "registration and registration access control", it is indicated that for

adequately manage the entry and exit flows and the traffic of people,

establish the following general measures: encourage online procedures and payments

and the replacement whenever possible of manual processes by digital ones,

sending accreditations online, downloading accreditations on the mobile, promoting

contactless media and manage queues with separator tapes.

FR technologies are also used to improve security. The MWCB is a

event classified as a “high security threat” by the Spanish authorities.

The verification of identification with FR is effective in achieving the objective pursued,

that is, security in a contactless environment.

Delegates who had chosen common or standard ID validation,

they used separate entry lines to those of the FR lines. They scanned your

digital pass and security staff compares the image stored on the pass

digital that was displayed on a screen in the appearance of the delegate. This was done to

some distance given the non-contact environment that the company considered little

likely to be as accurate as the identification check performed with

FR technologies especially in the context of trying to ensure a fast flow of

delegates to avoid overcrowding.

FR access identification checks were also faster, which

reduced waiting time and congestion within a closed space.”

Retained biometric data was deleted at the end of the event, only a few

weeks after registration and a few days after your treatment for control purposes

of access. These measures protect the data from being used for purposes other than the

identity validation.

The page that is included in “privacy policy” gives information about the process of

automatic identification validation, FR, leads to specific information about the

BREEZ (layers) and this page explains the possibility to choose verification of the

common identification, without the use of FR technology”.

Delegates have a real choice between checking their ID using-

do FR technologies or manually. The main difference between the two is that the option

tion FR allows the online registration process to be completed immediately,

while manual ID verification will require a short wait for

a few days to confirm the registration. This brief delay did not affect the ability

people to register for the in-person experience or delay participation.

tion at the event.

Data protection impact assessment

It is not provided, under the justification that "GSMA has carried out an evaluation

impact on data protection in relation to the use of FR technologies, and

this document is currently being reviewed in preparation for our event

MWC 2022."

International data transfers

The GSMA has a contract with a third party service provider (ScanVis Limited), who

It is not contributed, for the provision of FR services. “Our commitment against

with ScanVis includes the requirement to implement appropriate security measures

to protect the personal data processed by the service provider and conforms

to article 28 of the GDPR.”

SCAN VIS is based in Hong Kong, however the MWC FR data is hosted

two by Amazon Web Services (“AWS”) in Germany. How SCAN VIS is located

in an unsuitable country outside the EU, the GSMA has entered into contractual clauses

standard with SCAN VIS.

Also, as an added safeguard, biometric data is encrypted and only the al-

Gorithm itself can understand what it means.

The GSMA does not transfer personal data to Belarus or Russia, as disputed by the inter-

resada.

Appointment of an EU representative

“GSMA EVENT PROJECT MANAGEMENT, S.L. (EPM) is a Spanish subsidiary of

GSMA. EPM has been created specifically to provide services related to the

management of the MWC in Barcelona. Personal data processing activities

of the GSMA are inextricably linked to the activities of EPM.

Therefore, the GSMA processes personal data in the context of the activities of a

establishment of the EU and is subject to the GDPR pursuant to Article 3(1)

of the GDPR, so no EU representative is required in accordance with

compliance with article 27 of the GDPR.”

It does not provide the NIF of this entity, address or any identifying information.

FOURTH: In the Mercantile Registry (RM), a search is carried out under GSMA and it only appears

registered entity GSMA 4YFN EVENT MANAGEMENT S.L, CIF B67299297,

address Av. de la Reina Maria Cristina S/N Hall 1, Barcelona, corporate purpose

“Provision of conference and event services. Event organization

business, social, cultural, recreational or technological, including commissioning

March of trade fairs, etc." In the query to the AXESOR application, figure

as the sole partner of GSMA LIMITED. GSMA LIMITED is listed in the app

AXESOR as a non-resident entity, NIF N4004237F.

On the web https://www.dnb.com/business-directory/company-profiles.gsma_ltd.9e65a-aadc5cdd92b48292ac68a42aff7.html, it shows that GSMA LIMITED has 105 employees and $37.12 million of revenue.

FIFTH: On 09/21/2021, by application of article 65.5 of the LOPDGDD, The claim process continues.

SIXTH: On 06/9/2022, the Director of the AEPD agreed:

"START SANCTION PROCEDURE against GSMA LTD., with NIF N4004237F, for the alleged infringement of article 35 of the GDPR, typified in article 83.4.a) of the GDPR and article 73.t) of the LOPDGDD"

"For the purposes specified in the art. 64.2 b) of Law 39/2015, of 1/10, on Procedure Common Administrative Law of Public Administrations, the sanction that could correspond would be a fine of 200,000 euros, as specified, without prejudice to whatever results from the instruction."

SEVENTH: On 06/27/2022, the defendant indicates:

1) In its letter to the AEPD dated 09/10/2021, the GSMA provided detailed answers to the questions of the AEPD. The GSMA did not interpret the question regarding the Data Protection Impact Assessments ("DIAs") referred to the fact that the AEPD was requesting the contribution of a copy of said EIPD, but was asking confirmation that a DPIA had been carried out. According to this interpretation, The GSMA confirmed that it had carried out an DPIA for the use of facial recognition ("RF") and that the document was being updated for the MWC22.

They reiterate that the claimant did not register in the mode of use of "RF" technology, "due to Therefore, we do not consider that RF's EIPD was relevant for the purposes of this specific claim and it was interpreted that way".

2) They provide a copy of the EIPD of 01/12/2020 made using the "One Trust" system

"already existing when requested" and another that replaces it, updating it for the

MWC22. "The defendant did not ignore the need to mitigate the risks derived from the use

of RF technologies for the 2021 event", "which took into account the

information and evaluation of the aforementioned EIPD 2020" and "the need to minimize the

risk of spread of COVID-19", and took the following practical measures:

a) "the optionality of biometric data processing and the measures to

ensure that the manual identity verification option (without the use of

RF) was not to the detriment of the user;

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

18/48

b) "the provision of information related to the processing of biometric data in

layers and in a user-friendly way;"

c)

"the implementation of robust physical and technical security measures to stop

protect biometric data;"

d) "the imposition of robust security measures on ScanVis, the provider of

RF technologies, including safety assessments by the GSMA; and

e) "the deletion of the biometric information shortly, after the completion of the

event."

2) The impact assessment report, DATA PROTECTION IMPACT ASSESSMENT

(DPIA in English, EIPD in Spanish), of 01/12/2020, has the following characteristics:

-created on 12/17/2019, submission date 01/12/2020, name "MWC 20 process of

facial recognition", in English.

-Divides issues to be assessed, answering yes or no, and an explanation where appropriate.

It has 9 parts. The first: general part broken down into 9 questions, the second: identification of the parts that are part of the treatment and has 3 questions, the third: legality and transparency with 11 questions, the fourth: rights of stakeholders and accuracy, with 12 questions, the fifth: limitation of the purpose with four questions, the sixth: data minimization, with 5 questions, the seventh: storage limitation, with 5 questions, the eighth: integrity and confidentiality, with 11 questions and the ninth: additional information. The results that appear are 0 in all kinds of risks, residual risk, none. it has to mean:

a) In the first section: "general", it is indicated that "it is a new version of the process facial recognition system updated for 2020" (in which events are mentioned dated in Congress in 2020, none in 2021), and that BREEZ is the term customer-oriented for our facial recognition process." It is a review of 2019 project, which includes its changes since then, referring to:

-Development of a widget (device, application) of registration completely new you.

- The main promoted method of capturing photos is through a selfie to ensure that the captured photo is recent. Users can still upload a photo if necessary.

- Selfie capture includes real-time guidance and feedback for ensure that the face is in the correct position and is accepted by the FR algorithm. There are specific error messages to guide the user in case of BREEZ photo captured/provided being rejected.

- The enrollment widget also includes a verification check

of FR in real time to make sure that the person who registers can be re-

known to the system. The user can skip this step if necessary.

- BREEZ inscription promoted from within the photo upload process of

profile.

- Integration of a new widget that allows attendees to scan their

Passport/EU ID; this will extract the data from the machine readable zone (MRZ),

as well as the photograph in the identification.

- The captured photo of the passport/EU ID is compared with the captured photo-

given during BREEZ registration to determine probability.

- Inclusion of the concept of Secured Attendee Profile (SAP) which means

that through the automation process the wizard has:

a) provided your passport/EU ID details

b) has enrolled in the BREEZ FR program

c) the EU ID/Passport photo matches the photo provided for

BREEZ.

It indicates that in carrying out the DPIA its "team for the Protection of

data", together with the mention of article 35.2 of the RGPD that indicates the participation of the

Data Protection Officer.

The purpose of this process is to streamline manual processes at the site in the mo-

collection of credentials and provide an efficient service. (1.7 purpose of

the proposed processing operations.)

b) In the legality and transparency section, (3.1) it is indicated that the consent that

is the basis of treatment, it is requested freely, informed, specific and without

biguity, keeping the accreditation of consent. (3.3).

method for attendees to access MWC/4YFN.

a) in question 4.3, when the personal data is transferred to a third country

or to an international organization, the interested party will have the right to be informed

aware of the adequate safeguards provided by the person in charge or in charge

gado? and it indicates yes.

b) indicates in question 4.4 that: "all the biometric data collected for the

purposes of this project will be deleted as the end date of 03/26/2020" (not

However, the Congress of the year 2021 is being analyzed). The rest of the data in

In accordance with the data retention periods of 5 years will be stored, to

unless there is a request for its deletion."

c) In question 5.1 "limitation of the purpose" of the answer given, it is indicated

that: "those attending the Mobile World Congress have the opportunity to sign up

to the FR program until 02/27/2020".

e) In question 5.2, how would you assess the need for treatment operations?

proposals?, the answer is average, and the justification: "In order to satisfy the

security measures in the event, we have been instructed by the form of the

Spanish Police to put strict processes in place to ensure that all

attendees are screened through a passport/document check

EU identity cards before they can

- collect your badge-credential

- every time they enter the premises.

The above processes rely on manual verifications which can be slow and

provide a negative experience at the event.

Through the use of technology described in this DPIA, we may automate them to

allow much more use

efficient, as well as a more precise and safe event.”

f) In question 5.3, it is indicated: "if the proposed treatment operations are

proportional to its purpose?", Article 35.7 B is included in its wording, and the

answer is yes, indicating in justification that "to satisfy the requirements it is

necessary to create biometric tokens based on the photographs”.

g) In section 6, the number of subjects in the answer puts, high, more than 1000, and

that the information is collected in electronic format, online (6.3).

h) In section 7.4, it is indicated that the data storage period is

up to 5 years except biometrics.

In section 8 of integrity and confidentiality it is indicated that the data is

Yo)

stored in third parties being the format in text and images, and that the

biometric token is encrypted, backup copies are made of the data that is

created and maintained, and there is a trace of access to the data, including the

encrypted data-

2) The DPIA report document is also provided, "updated to 06/27/2022",

“reasons for upgrade: refers to the previous one of the “one trust” system, using

now a different format that includes more information.

Part A-information on the projected treatment, is structured in 14 parts:

First, it answers the questions of purpose and how the system works.

To process biometric data obtained from the use of FR-recognition technology

facial- during the registration process for the event before attendance and during the

access control. “The main reason to use FR is to ensure that the GSMA needs

a high degree of security together with contactless access and fast track access to the

event to minimize the risks of spreading COVID 19. The technology will use the

measurement of face points (distance between eyes or from forehead to chin) for

verify the identity of the person through a biometric model. They are treated a

number of data points to create a map of the person's face in time

real. This is converted to a secure template model, using a complex algorithm

to create the “biometric token”. “For security purposes in access to the headquarters,

GSMA will automatically check the image taken at the access point against the

“biometric token”, stored in its database. are included in the treatment

third parties, SCAN VIS, the provider of the FR technology. The data

Biometrics are obtained before the event, during registration. Provide in annex i a

diagram detailing the data collection process in which it appears that "For the

registration uses the JEMEX REG SYSTEM software that allows third-party integration

parts in addition to uploading documents, as in this case, "the user has to upload the

passport" and the software a portrait photo, checking whether the image

It is readable by the system.

Biometric data is stored in the European Union on servers of

Amazon in Germany and Spain

The second issue is the data of individuals that is collected at the level of

categories number of individuals and geographic area.

The third question is the type of data that includes the question of why they are requested,

indicating that the passport and biometric data have the purpose of "confirming the

identity and to be able to enter the event". Being the source of origin "the same people".

-If special data is processed, indicating yes, in biometric data "ID

verification and access control"

5-"service providers": refers to SCANVIS that manages the FR service, that

provides a web application "included in the data exporter registration system and

Using this dieget data importer will help a data exporter to collect a quality verified phase

phto/profile photo through the widget . ScanVis is located in Hong Kong, some

of its employees are located in China, but are subject to the policies of

ScanVis, including the security policy on data protection.

"ScanVis has contracted Amazon servers to store the data

biometrics that it deals with when it provides services to the respondent. amazon act

as a sub manager. ScanVis access to Amazon servers is remote

and sporadic, only when there is a technical matter.

ScanVis can gain access when there is a technical issue with the biometric tokens.

6- "other disclosures to third parties" It is indicated that each year prior to the

celebration of the MWC, the Mossos d`Esquadra, send a letter requesting the

requested to provide information regarding attendees: first name, last name and

Passport number of attendees. Biometric data is not shared with

the Mossos d'Esquadra. The request is carried out under a security plan the plan

security director of the Mobile World Congress, to which they do not have access.

The seventh the information that will be provided to people

The eighth individual rights and options

The ninth, marketing communications

The tenth ,automatic data collection

The 11th retention period

The 12, destruction

13, security

the 14th, others

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

The second part refers to the risk assessment methodology, divided into

part b 1 "Methodology" which starts from the fact that "once the risk has been identified, it is

essential to qualify the probability of it happening-probability- as well as the level of

impact that its materialization entails-severity. “”This quantification depends on the

description of the treatment, the circumstances and the means in which it is carried out”.

Attach some probability/severity color boxes, with the values very low,

low, medium, high and very high

Part b.2, “two” “requirements to carry out a DPIA”, is divided into:

Obligation to file a DPIA

Assessment of the need, suitability and proportionality of the treatment

Part b 3 "risk assessment" has a table that indicates: "probability-

identify the probability of the materialization of the identified risk, considering the

treatment and the measures taken for the design and the defect", stating in all

they low, or very low, in "severity" some sections have "high", the "risk

resulting from combining probability and severity", consists of medium and low and the last one, of:

"Identify how the risk can be mitigated", stating that it is not necessary or that

is mitigated. It is subdivided into 23 sections -not all of them are cited-, highlighting:

1-Responsibility for compliance.

2-Roles in treatment

3-DPO and representatives

4-Legality

5-Information notices

6. Legitimizing bases

7-Limitation of purpose

8-Data quality and minimization

9-Data retention

10 Rights of people

11- Automatic decision making and profiles

12- no content

13-Security

14- Data export

15-Compliance with the policy

20 privacy by design and default

It ends with a table in one column "type of recommendation", in the other,

"recommendations".

In type: "Legal recommendations", review of the DPIA in an annual scheme

considering that legal teams monitor withdrawals of consent,

their levels, and the number of complaints and suggestions that could mean that there has not been

understood the language of consent, these are currently very low. Review

also the Privacy Policy and the FAQS on data processing

biometric,

“Organizational recommendations”: include policy implementation,

training, and audit measures, In recommendations: to audit the

rights in the ScanVis contract and verify compliance with the contract, e.g.

example contemplating the provision of confirmation of data erasure in writing

at the end of the contract, and carry out verification or monitoring of employees

with the current Data Protection policies

“Product Recommendations”, defined as those that require implementation

technique, anonymization measures, menu settings, contextual notes,

figure without recommendations, and

“other recommendations”, that are not included in the previous ones, nothing appears.

EIGHTH: On 12/20/2022, a resolution proposal was formulated, with the literal:

"That the Director of the Spanish Agency for Data Protection sanctions

GSMA LIMITED, with NIF CIF N4004237F for a violation of article 35 of the

GDPR, in accordance with article 83.4 a) of the GDPR, and for prescription purposes

in article 73.t) of the LOPDGDD, with a fine of 200,000 euros.”

NINTH: On 01/10/2023, there was a written entry of allegations in which it indicates:

1) Mention Directives 4/2022 of the European Committee for Data Protection, CEPD

“European Data Protection Board (EDPB), “on the calculation of administrative sanctions

Treatments”, which are displayed on the web https://edpb.europa.eu/our-work-tools/our-

documents/publication-type/guidelines_es, in "public consultation period", from

05/16/2022 to 06/27/2022, without having been adopted yet. It states that in

they analyze in detail each of the circumstances of article 83.2 of the

GDPR.

Indicates that the proposal does not consider any mitigation, and asks to review and moderate the

applicability of aggravating circumstances.

2) It requests that they be considered as mitigating factors, in order to reduce the amount of the penalty.

tion:

2.1 "Article 76.2.a) of the LOPDGDD establishes as a circumstance to assess

the continuing nature of the offence. In the present case, the data processing obtained

subject of the impact evaluation had a very limited duration in time: specifically

It began on 03/22/2021, the date on which the registration to the MWC Barcelo-

na 2021 (“Event”) where you could opt for facial recognition (“RF”) and ceased

four weeks after the end of the Event (on 07/29/2021), at which time the

deleted all biometric data collected. In total, the data processing

It lasted approximately four months. We consider that it is

a short duration and that this fact should be taken into account as mitigating the in-

fraction."

2.2. "Article 76.2.f) of the LOPDGDD establishes as a circumstance to assess

affecting the rights of minors. The professional and netwo-

rking of the Event means that it is addressed to adults related to the field of

the technology. These people have -predictably- technological knowledge for

above the average citizen, and they are specially trained to decide for themselves

themselves if they wish to choose the RF option as the registration method for the Event. In

very rare occasions (for example, when an assistant cannot get someone to

someone stays in the care of your child) data of minors is managed. The

Minors are registered following a separate process, as escorts.

tes, and are excluded from the registration system by RF. We can confirm that it is not

has used RF with any minors. “

23. "Article 83.2.e) RGPD establishes as a circumstance to assess any in-

previous fraction committed by the person in charge or in charge of the treatment. I gave them-

guidelines 04/2022 consider that the existence of previous infractions should be assessed,

paying special attention to the temporality and the matter of these. Since 2006 when

GSMA held the Event for the first time in Barcelona, none have been registered

violation of data protection regulations sanctioned by the AEPD. Considers-

We note that the fact that it is a first infringement is especially relevant.

taking into account that the GSMA has been organizing large-scale events for 16 years

dimensions in Spain and that, up to now, no misconduct has ever been committed.

fraction, which demonstrates the commitment and involvement of the GSMA in relation to the

compliance with the regulations on the protection of personal data”

2.4. "Article 83.2.e) GDPR establishes as a circumstance to assess the degree

cooperation with the supervisory authority in order to remedy the infringement and

mitigate the possible adverse effects of the infringement. The GSMA is clearly committed

mind for transparency and collaboration with public administrations, in

In this specific case, GSMA has been at the disposal of the AEPD and has responded to the

information requirements in the best possible way, facilitating documents and

information relevant to the case. In addition, in this sense, and without there being

been required by the AEPD, information has been provided on the new evaluation of

impact carried out with the intention of complying with the regulations and correcting non-compliance lie in future events".

3. "About the aggravating circumstances of articles 83.2.a) and 83.2.b) GDPR that apply in the resolution proposal, we request that they be reviewed and their applicability assessed in the specific case taking into account the following arguments:

3.1. The resolution proposal considers, regarding the aggravating circumstance of article 83.2.a) GDPR, that "the data of a very high number of attendees was processed (20,000 people), without considering the level of high risk, in relation to the affectation to their rights and freedoms, which may exist for treatments based on face recognition". On this aspect it corresponds to indicate that the RF was offered as an optional registration measure and that, according to the information provided According to our registration systems, the RF was only used by 7,585 people.

We request that this number be taken into account for the valuation of the amount of the sanction. It also corresponds to indicate that there has been no record, not even during the time that the treatment was carried out, nor after the damage occurred or damages or any affectation to the rights and freedoms of the interested parties.

3.2. The resolution proposal considers, regarding the aggravating circumstance of article 83.2.b) GDPR, that there is no evidence that the entity has acted

intentionally, although the action reveals a serious lack of diligence in his conduct in adopting precise proactive measures in such a unique regime, differentiated and special data applicable to the type of data processed, without it being stated that

They have put the basic means so that it did not occur. The performance to which the resolution proposal refers to is the breach of article 35 itself of the GDPR. No additional circumstances are described or listed that may valued to justify the applicability of this aggravating circumstance. In this regard, the GSMA has submitted information that demonstrates diligence in the treatment performed, the application of robust security measures imposed on service providers RF services and the existence of adequate contracts with all of them. In this sense, we do not agree that there is negligence in the infringement and we consider that the violation of article 35 of the GDPR, by itself, cannot entail the applicability of the aggravating factor of negligence.

4-Ends by indicating that: "requests that the AEPD reconsider the proposal for resolution and proceed to warn or reduce the amount of the sanction".

NINTH: Of the actions carried out in this procedure and of the documentation in the file, the following have been accredited:

PROVEN FACTS

1) In the terms and conditions of attendance for the MOBILE WORLD CONGRESS (MWC) of Barcelona 2021, it appears that GSMA Ltd. ('GSMA') is the entity organizer of the MOBILE WORLD CONGRESS (MWC) of Barcelona 2021, to celebrate between 06/28 and 07/1/2021, and performs, among others, data processing of the assistants. The website www.mwcbarcelona.com/legal contains information on the Barcelona 2022 Congress, indicates that "GSMA LTD with its main place of business located in Atlanta, USA, wholly owned subsidiary of the association GSM, and with respect to 4yfn 2022, GSMA 4fyn EVENT MANAGEMENT S.L., a subsidiary of GSMA LTD., welcomes you to MWC BARCELONA 2022.", and that "GSMA LTD and its affiliates provide you with the event…" According to information from

internet, GSMA (Global System for Mobile Communications, “Global System for

Mobile Communications), is an organization of the mobile industry that brings together

operators from all over the world, more than 750 mobile phone operators and more than 400

Companies are associated as members.

According to the defendant: GSMA EVENT PROJECT MANAGEMENT, S.L. (EPM)

is a Spanish subsidiary of GSMA. EPM has been created specifically to provide ser-

vices related to the management of the MWC in Barcelona. The trafficking activities

GSMA personal data processing are inextricably linked to the activities

EPM lives.

Therefore, the GSMA processes personal data in the context of the activities of a

establishment of the EU and is subject to the GDPR pursuant to Article 3(1)

of the GDPR, so no EU representative is required in accordance with

compliance with article 27 of the GDPR.”

The aforementioned entity is not registered in the Commercial Registry, if it does include: GSMC

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

EVENT PROJECT MANAGEMENT, S.L., Cif B64828973 and as a corporate purpose: "the

provision of project management services, and support services in relation to

with the conferences, congresses, shows and meetings organized by any

of the companies belonging to the group of the companies belonging to the group”

On the other hand, the entity GSMA 4YFN EVENT MANAGEMENT S.L, CIF B67299297,

address Av. de la Reina Maria Cristina S/N Hall 1, Barcelona, has a corporate purpose

“Provision of conference and event services. organization of company events

commercial, social, cultural, recreational or technological, including start-up of

trade fairs, etc." In the query to the AXESOR application, it appears as a partner

only GSMA LIMITED. GSMA LIMITED appears in the AXESOR application as en-

non-resident entity, NIF N4004237F

2) In the terms and conditions of assistance, the registration process that

would allow face-to-face access for those attending the event for that 2021, it has been

to create an account on your website, and register for support, so that when

Arriving at the physical headquarters, you should already be registered. At headquarters there would be no areas of

registration support and paper credentials would not be provided. The system intended

have verification of identity collected prior to each person's arrival at

headquarters. For the year 2021, the MWC provided as mandatory in the modality of

face-to-face attendance at your headquarters, the registration of the DNI/passport, identity card,

uploading it to your website. Only it was not required to upload the identity documents to the

who opted for the “virtual” modality. These requirements are contemplated in Clause

of "general terms and conditions for attendance" MWC 2021, Barcelona" in the

that attendees have to accept these conditions.

In the terms and conditions of assistance, it is provided "Identification: You agree to arrive

var a photo identification issued by your government in the form of a passport or card

EU national ID card with you at all times during the Event. HE

You will be asked to present such identification. You are solely responsible for the accuracy

of all personal data provided when registering for the Event…”

In addition, data such as "name, position, name,

company name, work address, work email, job functions, phone number

telephone, area of interest and photograph. If you are a speaker, as additional information,

your professional profile

3) The defendant indicated to the claimant that the passport and identification data

are required and are demanded by the Mossos d`Esquadra, that the legitimizing basis for the treatment of uploading passports and identity cards is article 6.1 c) of the GDPR inasmuch as they were required to provide certain information to the Mossos: name surname nationality date of birth identity document provided date of issue and document number, this being the way of provide it novel, for being electronic and "that has changed by 2021, due to that businesses need a contactless environment." The defendant does not prove this requirement or that it should be through a website, of its own private ownership, where they are collected and stored. The defendant pointed out that in previous editions of the Congress, the assistants carried their identification cards in a credential.

4) In general terms and conditions for attendees it is indicated in privacy and

Data Protection that data is collected "about you in connection with the provision of the services and for account management" and that more details about the privacy policy practice on the processing of personal data is available in Privacy Policy-city. The Privacy Policy indicates that information about the data is obtained collected from various groups, among others, attendees, through the system of registration of attendees, the event app, digital and/or printed credential cards, or the facial recognition scanning system (at access points, to se-sessions or to participate in closed space meetings). It indicates: "information that you voluntarily provide: "when… you create an account with us, you register after the event, ...you require a service…""The information collected includes, but

It is not limited to: your name, title, company name, work address, email

job, job functions, phone number, area of interest, and photograph. If you're

a speaker, as additional information, your professional profile”

5) The defendant explains that after taking the aforementioned identity documents,

there is the possibility when you register on the web, for face-to-face access, of two

modes, and one more residual:

a) Automatic verification recognition, also called verification validation

automatic identity: Together with the identity documents already uploaded, the automatic identity

The website of the defendant requests the express consent to use BREEZ (acronym for

easy entry with biometric recognition) that uses facial recognition

biometric . In this modality you can enroll both during registration and

after registering for the event. The BREEZ system assumes that the

SCANVIS software -responsible for the treatment of the claimant- takes a photo of

the person automatically matches the image “provided to us with the

photograph in their passport/national identity card”, “to whom it will attribute some

matching scores”, “the technology analyzes facial features, taking

measurements of the data points that make up the face, such as distance between eyes, or

from forehead to chin, a series of data points are processed to create a

map of your face in real time, this is converted into a data pattern using a

algorithm to create what the defendant calls a "biometric token" (biometric file,

identifier). This token is what makes it possible for your captured image to be accessed

by the FR reader matches and the event is accessed in its own differentiated queues,

for sessions or to participate in meetings in closed spaces or even areas

restricted.

In the non-contact accesses with BREEZ, it is indicated that "it will verify your image

captured by cameras against your biometric token for validation purposes

of identification”.

The consent information in BREEZ states that “You consent to

GSMA using your biometric data obtained from photographs provided by

you for identification validation purposes in the context of online registration

and for the MWC Barcelona for the purpose of accessing the venue”, preceded by a

chair that indicates "Yes, I consent to the use of my biometric data for self-validation

identity mathematics”.

It bases the purpose in a double sense, to verify the identity when attending the

event, and security in the access to the enclosure. The legal basis of this treatment according to

indicate it would be express consent, being able to withdraw their consent with what

its validation would become manual.

Information on the BREEZZ system is expanded in the BREEZ FAQS -FR section

The consent granted for the automatic validation of the identity can be

withdraw at any time

a) Recognition of manual verification, or manual validation of identity:

Together

to the identity documents already uploaded, the web program of the claimed

Take a photo of the attendee. It implies that access will occur with

control through human presence, which performs the verification when the assistant

when approaching, he scans his digital credential in the form of a QR reading, showing the

photo taken that sees the human presence at the same time as the person.

b) Exceptionally, validation of identification on paper, face-to-face on site

2) The one called by the defendant: "biometric token" created for the process of

image comparison will be removed four (4) weeks after completion

of the event. Check the section How is my biometric data used and stored?

that each biometric token is encrypted and stored in a separate database from the

raw data used in its creation

However, in the BREEZ FAQS it is indicated that although it has no contact,

all attendees must have their digital credential available to enter the

external perimeter of the place and that the digital credential will also be the only way to

access conferences and their partner sessions.

3) According to the defendant, the SCANVIS entity with which it has an assignment

treatment of the facial recognition system for access to the headquarters,

located in a country outside the EU, and the GSMA has entered into contractual clauses

standard with SCANVIS. It adds that the MWC FR data is hosted by Amazon

Web Services (“AWS”) in Germany.

4) The defendant stated that at MWC 2019, she allowed paper copies of

identification documents will be manually verified when accessing the headquarters of

MWC, an option that in 2021 was suppressed -with some exceptions- for reasons of health and

security, in order to minimize the risk of spreading COVID-19,

reducing queues and crowds at access points. This is in line

with the "action plan for congresses of the Generalitat of Catalonia" to which it is subject to

the GSMA and that expressly requires the replacement of manual processes by processes

digital.

5) According to the claim to MWC 2021, approximately 20,000 people attended.

10) Before the 2021 MWC, the defendant had a document of

IMPACT ASSESSMENT that is provided in allegations, entitled: "MWC20

Facial recognition process", created on 12/17/2019. It has nine sections with

answer yes/no, related to the principles of data protection, appearing zero

in all kinds of risks, residual risk, none. In several issues he reproduces the

GDPR article, and the answer: Yes (example 4.5, 4.4, 4.6 among others) In the first

section: "general", it is indicated that "it is a new version of the

updated facial recognition for 2020" (in which events dated

in Congress in 2020, none in 2021), and that the "term BREEZ is the term

customer-oriented for our facial recognition process." It is a review of

2019 project, which includes its changes since then, referring to the

BREEZ performance. In the section How would you assess the importance of

need for treatment operations? (5.2) does not indicate the activity of

treatment of facial recognition, indicating: "In order to satisfy the measures

security at the event, we have been instructed by the Police Form

Española to put strict processes in place to ensure that all

attendees are screened through a passport/ID check

EU identity card before they can enter the venue, and collect their

credentials. Legacy processes are based on manual checks that

they can be slow and provide a negative experience at the event. Through the use of

the technology described in this DPIA, we may automate them to enable a more

much more efficient process, as well as a more accurate and secure event."

In section 5.3 on the proportionality of processing operations, only

indicates that yes, "to satisfy the requirements, it is necessary to create tokens photo-based biometrics. The document lacks an evaluation of the necessity and proportionality of processing operations with respect to their purpose; the use of facial recognition for access to events, of your assessment of risks to the rights and freedoms of the data subjects to which referred to in section 1 of article 35 of the GDPR and of the measures planned to deal with risks, including guarantees, security measures and mechanisms that guarantee the protection of personal data, and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of the data subjects and other affected people. Likewise, it relates the data of the passports and cards of identity that he manifests are required by the Mossos d`Esquadra that allegedly have a purpose, to connect it with the photo that is taken with the software, that initiates the facial recognition process, matching your identity to facilitate the access.

FUNDAMENTALS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), grants each control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter, LOPDGDD), is competent to initiate and resolve this procedure the Director of the Spanish Protection Agency of data.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures processed by the Spanish Data Protection Agency will be governed by the provisions in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations dictated in its development and, insofar as they do not contradict them, with character subsidiary, by the general rules on administrative procedures."

II

According to the terms in which the claim is formulated, it is always mandatory Before going to the Congress, its headquarters and its events, register at the website of the claimed party, so when you arrive you must already be registered. It It is carried out with the creation of an account and the registration on the web of the claimed party. It is mandatory in general, when the registration on the web is attended in person with the introduction on said website, in the form of uploading the document (ID card, or passport, for security reasons required according to that claimed by the Mossos d`Esquadra, and a photo for identification purposes at the accesses of the event, documents of identification, which the previous year were presented or exhibited, this 2021 they will be uploaded to the web and are made on the web.

The defendant values the fact that the uploading of said identity documentation (DNI and or passport identification document) is required by the Mossos d`Esquadra, included in article 11.1.h) of Law 2/1986, of 13/03, on Security Forces and Corps Security, which would indicate:

"1. The State Security Forces and Bodies have the mission of protecting the exercise of rights and freedoms and guarantee citizen security through the performance of the following functions.

[…]"

a) Capture, receive and analyze any data of interest for order and security.

public ity, and study, plan and execute the methods and techniques of prevention of

crime”

This requirement in data processing has not been specifically analyzed in this

procedure, but if it is indicated by the defendant that for this 2021, this process has

changed, “being provided electronically”, “by the contactless environment”. Seems

It may be that in other years these documents were shown when accessing the premises, limiting

partly the intrusion that the processing of these data supposes to their owners the

have to upload them to a website owned by the claimed. In 2021 it was mandatory, not pa-

considering that, for convenience, data can be collected that could be excessive,

when before there was room for a mere exhibition of the document, especially in the case of documents

official identification documents, which, as well instructed, also “must carry

people at all times

Nor is it clear how it transfers the identifying data it collects from each

assistant the one claimed to the Mossos d`Esquadra, if he delivers the identification document

that attendees upload the claimant's website and the photo, or only give the data that

precise, which would oblige her to extract them one by one by people dedicated to it.

When trying to promote non-contact due to the pandemic, instead of displaying the document,

the defendant keeps a copy of it.

In any case, the defendant should reassess whether she has legitimacy for this

treatment activity.

In addition, the Congress attendee is given a credential or digital card that

contains your data. The assistant in virtual mode, not face-to-face, was not required to

previous identification in the form of providing ID, identification document or passport.

The common modality of registration in terms of access is manual validation, which

Based on the upload of the aforementioned documents, and the photo, recognition does not apply

facial. The person who attends the event accesses carrying his credential that he carries and

sample and scanning it, an employee verifies that the accessing person matches

that of the photograph and the documents that it bears in the credentials

Another method of registering and accessing involves entering the same data, but

giving consent, marking a box for it, which would associate the same

documents for an easy entry mode, through recognition

facial biometric. This identification is produced, not only by introducing the document

public identification of the person on the web as a way of identifying themselves, which in

if it is not biometric data, but based on a photo taken by the software, which

compare with the photo of the identity document-passport, and after taking

perform a specific technical treatment: transformation by means of an algorithm on

points of the face, converting them into a template, or biometric token, as

name the claimant.

In this way, with the passport, or DNI, as mandatory, with no alternative, plus the

facial recognition, we proceed in a bivalent way to an identification with double

joint factor, using facial recognition for contactless access and

more agile to installation. It ensures that it is that person by the uploaded documents

to the web and by the biometric template that manages the same web of the one claimed to

through a treatment manager.

On the other hand, in treatments without facial recognition, it is also saving

the photo, which is unknown if it is also managed by SCANVIS in its program that

is on the claim website, and if any pairing is made with the

passport/DNI in order to verify coincidence thresholds to deduct the

identification of the assistant who enters manual mode carrying his credential.

The claimant seems to encompass any physical access as linked to the data

Biometrics and their use. However, despite stating that he did have to raise the

passport, does not certify the use of biometric data, and the defendant asserts that it does not

used this modality, noting that "he registered as a virtual assistant and took part

as a speaker at a roundtable" and "was not required to download or upload document

of identity".

II

The scope of application of the GDPR extends its protection, as established in its

Article 1.2, to the fundamental rights and freedoms of natural persons and, in

In particular, your right to the protection of personal data, defined in its article

4.1 as “any information about an identified or identifiable natural person (“the

interested"); An identifiable natural person shall be considered any person whose identity

can be determined, directly or indirectly, in particular by means of an identifier,

such as a name, an identification number, location data, a

online identifier or one or more elements of physical identity,

physiological, genetic, psychological, economic, cultural or social of said person.”

The defendant has processed personal data, and specifically data

biometric. The concept of treatment The GDPR defines in its article 4:

"2) "processing": any operation or set of operations carried out on

personal data or sets of personal data, either by procedures

automated or not, such as the collection, registration, organization, structuring,

conservation, adaptation or modification, extraction, consultation, use,

communication by transmission, diffusion or any other form of authorization of

access, collation or interconnection, limitation, deletion or destruction;

7) "responsible for the treatment" or "responsible": the natural or legal person,

public authority, service or other body which, alone or jointly with others, determines the

purposes and means of processing; if the law of the Union or of the Member States

determines the purposes and means of processing, the controller or the

Specific criteria for their appointment may be established by Union law

or of the Member States;

Biometric data as specific types are defined by article 4.14 of the GDPR:

“personal data obtained from a specific technical treatment, related to

the physical, physiological or behavioral characteristics of a natural person who

allow or confirm the unique identification of said person, such as facial images

or dactyloscopic data;

The special categories of data referred to in article 9 of the GDPR establishes:

"1. The processing of personal data that reveals ethnic origin is prohibited

or race, political opinions, religious or philosophical convictions, or affiliation

union, and the processing of genetic data, biometric data aimed at identifying

unequivocally to a natural person, data relating to health or data relating to

sexual life or sexual orientation of a natural person.”

In this case, those who consented to the use of facial recognition were given a

photograph by the program on which the specific technical treatment is produced

which ends in the creation of the biometric template through the application of an algo-

rhythm.

Thus, the biometric information collected (for example, the image of a fingerprint

fingerprint) is processed following procedures defined in standards, and the result

of that process is stored in data records called signatures, patterns, or

"templates". These patterns numerically record the physical characteristics that

allow to differentiate people, they are data of the person, not about him, they constitute a

form of reduced mathematical representation of the original feature. express

uniquely and compactly the identity of the individual. Raw data is not stored

cough but an extract of its characteristics.

The biometric pattern extracted by the registration module is stored in the database

recognition system data. The biometric pattern is stored for your

comparison. The database will therefore contain all the biometric patterns

of individuals who are legitimate users of the system. Also, depending on

application, said pattern could be stored on other supports, such as

For example, a magnetic card or a smart card (match-on-card and match-on-card techniques).

on-token). In these cases, the data is stored exclusively on the support

card, there being no centralized database.

The biometric data system, in the identification or verification process, does not seek

eventual equality between the sample and the stored data, but has as its

The objective is to find enough matching points to determine that there is a

coincidence, not equality. This is recognized by the defendant when indicating that the

photo taken with the passport photo, establishing a high match threshold

to continue the process in the creation of the template.

In the last phase of the process, a biometric sample will be compared -such as the face-

presented to the sensor with a pattern that appears in the database of the claimed.

The definition of biometric data includes that through technical processing

I specify, "allow or confirm" "the unique identification" of said person. The

Mentions to "allow" can be understood to the identification, that of "confirm" to the

check. Therefore, both identification or authentication must be unique,

referring to the identification that occurs of the person. The unique identification by

On the other hand, it goes beyond the fact that the data is from an identified natural person or

identifiable. Identified natural person data is that that person is distinguished or

isolates from a group of people. Unique, can refer to that biometric data

have such particularities that they can unambiguously identify an individual

In the present case, of course, it cannot be said that information is not being

linked to personal data of a person identified in each access to the headquarters in

face-to-face mode, even if the data is saved on the device encrypted/encrypted.

Every time an attendee stands in the vicinity of the entrance, in front of the specter that

reach the camera, allows or confirms your unique identification through the treatment

carried out by the claimant with the devices purchased and through technology

of software implanted. The submitted sample is compared and the system has the

identification function with a biometric function, uniquely identifying the

assistant who claims to be and registering your data.

Biometric data present the particularity of being produced by the user himself.

body and definitively characterize it, are data not about that person, but rather

data refer to the same person, in principle not modifiable by will of the

individual, nor the person can be released from them, they cannot be changed in case

compromise-loss or system intrusion. Furthermore, because the data
biometrics are typical of a person and perpetual, the user uses the same
data in different systems. Therefore, identity theft is not only perpetual in
time, but affects all systems in which a user has stored
your biometric data. Therefore, the owner does not have the possibility of using data
biometric for the bank, and a different one for your health system, but uses the
same information to verify your identity in both, and against a vulnerability
they are all affected at the same time. Finally, the interested party does not know
that your information is being used, being able to obtain through objects,
traces or surveillance cameras.

Recitals 51 and 75 of the GDPR refer to spatial data, "a group of
personal data which, by their nature, are particularly sensitive due to the
significant risk that they may entail, in the context of their treatment, for the de-
fundamental rights and freedoms. The common denominator of all of them is that their
processing involves a significant risk to the fundamental rights and freedoms
mental since it can cause physical, material or imma-
terials. This group or category of particularly sensitive data includes the
categories of specially protected data regulated by article 9 of the GDPR -with-
recital 51 of the GDPR- and, in addition, many other data not regulated in that precept-
to. Recital 75 mentions in detail the personal data whose processing
may entail a risk, of varying severity and probability, to the rights and

freedoms of natural persons as a result of the fact that they can cause damage and

physical, material or immaterial damage. Among them he mentions those whose treatment

behavior "may give rise to problems of discrimination, identity theft or

fraud, financial loss, damage to reputation, loss of confidentiality of

data subject to professional secrecy, unauthorized reversal of pseudonymization or

any other significant economic or social harm;" (The underlining is ours)

Recital 51 of the GDPR refers to the systematic non-consideration as

a special category of data treatment, to the photographs, unless they are

apply a specific technical treatment means that "allows the identification or

univocal authentication of a physical person".

They are named that way because their treatment involves situations in which

a serious risk of data protection arises, from the consequences that its use

may have for people, and they are considered so harmful that their treatment

behavior is prohibited unless an exception applies, in which case the behavior

express feeling.

In addition to the circumstance that lifts the ban on

treatment, one of the legitimate bases must concur so that the treatment of

data is lawful, which are defined in article 6.1 of the GDPR, and comply with the

principles that are expressed in article 5 of the GDPR, among which play an important

role the minimization and proportionality and need for treatment of these data.

In this case, reference is made to the basis of consent to lift the ban on

treatment, also existing, according to the defendant, the option of not using the

RF system, without suffering access restrictions.

IV.

Article 7 of the Charter of Fundamental Rights of the European Union, proclaimed

given by the European Parliament and the Council of the European Union and the Commission of

12/7/2000, prescribes that every person has the right to respect for their private life, and the

article 8.1 that everyone has the right to the protection of personal data

that concern you. Interpreted together, it is inferred that it can constitute a

violation of such rights any data processing by a third party,

in this case the one claimed. This use of the data of the people who attend the

event organized by it, under its conditions in which it establishes the means and the end

by which the data processing is carried out, supposes an intrusion of his right

to private life and data protection if it is not justified. Article 8.2 of

The Charter of Fundamental Rights specifies that personal data is only

They can be processed with the consent of the interested party or by virtue of another foundation.

legitimate element provided by law. In addition, articles 7 and 8 of the letter are not absolute.

admitting limitations, as long as they are provided for by Law, respect the content

essential nest of those rights and with observance of the principle of proportionality,

are necessary and respond effectively to objectives of recognized general interest

by the Union or the need to protect the rights and freedoms of others

(Judgment of the Court of Justice of the European Union, fourth room, judgment of 15

October 2013, C/291/2012.). These aspects, moreover, are reiterated in relation to

tion with fundamental rights, in art. 52.1 in fine of the Charter of Rights

Fundamental rights of the EU

Facial recognition processing presents high risks to the rights and

fundamental freedoms and before implementing a data processing project,

as long as it is probable that it poses a significant risk to the

rights and freedoms of people, it is necessary to audit its operation, not

in isolation but within the framework of the specific treatment in which it will be used. Gives-

Given the potentially detrimental consequences for the people affected, de-

more stringent requirements will have to be met in the impact assessment process of

any measure that interferes with the dignity of a person, in terms of issues

tion of necessity and proportionality, as well as the possibilities of the

individuals to exercise their right to data protection

This is ruled in:

- Section 72 of Guidelines 3/2019 on the processing of personal data

through video devices, of January 29, 2020, of the CEPD, indicates: "The use of

biometric data and, in particular, facial recognition carry high risks

for the rights of the interested parties. It is essential that the use of such

technologies take place with due respect for the principles of legality, necessity,

proportionality and minimization of data as established by the GDPR. Although the

use of these technologies can be perceived as particularly effective, the

Data controllers must first assess the impact on data controllers.

fundamental rights and freedoms and consider less intrusive means of achieving

its legitimate purpose of processing. “That is to say, it would be necessary to answer the question of whether this

biometric application is something that is really essential and necessary, or is it just

"convenient".

-Opinion 2/2017 on data processing at work, from GT 29, establishes

that "Regardless of the legal basis of said treatment, before its beginning

A proportionality test must be carried out in order to determine if the treat-

treatment is necessary to achieve a legitimate purpose, as well as the measures that must be

be adopted to guarantee that violations of the rights to private life and

secrecy of communications are limited to the minimum

Since in the 90s of the last century our Constitutional Court adopted the

called the "German test" in the examination of the principle of proportionality, is a

constant in its jurisprudence, that the measures that affect rights

essential, they must be suitable or adequate, necessary and proportionate in

Strict sense.

-The Working Group of article 29, GT29 (adopted on 06/08/2017) (created by virtue

of article 29 of Directive 95/46/EC, independent European advisory body on

matters of data protection and the right to privacy, whose duties are described

in article 30 of Directive 95/46/EC and in article 15 of Directive 2002/58/EC,

assumed today by the European Committee for Data Protection, CEPD), in its Dictation-

men 3/2012 on the evolution of biometric technologies, indicates that "When analyzing

the proportionality of a proposed biometric system, it is necessary to consider previously

mind if the system is necessary to respond to the identified need, that is,

if it is essential to meet that need, and not just the most suitable or cost-effective. A

The second factor that must be taken into account is the probability that the system will be

effective in responding to the need in question in light of the specific characteristics

details of the biometric technology to be used. A third aspect to consider

is whether the resulting loss of privacy is proportional to the expected benefits. Yeah

the benefit is relatively minor, such as increased comfort or slight savings,

then the loss of intimacy is not appropriate. The fourth aspect to evaluate the

adequacy of a biometric system is to consider whether a less invasive means of

intimacy would achieve the desired end".

These assessments require exhaustiveness, starting in this case, not only from the

prohibition of treatment of these data, but considering the risks of using a

intrusive technology, biases or the likelihood of misidentification, its

interoperability, spoofing and unique identity type,

permanent and invariable that are treated, their impact on the privacy of people,

the fundamental rights implications of such systems and the

security measures, its increasingly widespread use, and technological interconnection is

more likely to interfere with these fundamental rights and may lead to

can lead to

serious violation of rights.

serious violation of rights.

Data controllers must ensure that the assessment of the need and

proportionality consider a thorough assessment of alternative options

less intrusive available. Therefore, the feasibility of

other available alternative options that do not require the use of special data,

compare all options and document the conclusions. All this, considering

the context of the framework in which the treatment is traced, compliance with the

obligations through the record of working hours.

The necessity implies that a combined evaluation, based on facts, is required.

on the effectiveness of the measure for the objective pursued and on whether it is less

intrusive compared to other options to achieve the same goal

Need should not be confused with system utility. It may be easier to not

having to carry a card, is automatic and instantaneous and not excessively expensive.

Obviously, an RF system can be useful, but it doesn't have to be objectively

necessary (the latter being what should really be present). as it establishes

Opinion 3/2012 on the evolution of biometric technologies - of GT 29-,

must be examined "if it is essential to satisfy that need, and not just the most

suitable or profitable. Regarding the reliability of the system, it must be said that how much

the greater the number of identification systems that are based on biometric data

or in a template obtained from biometric data, the greater the risk that

This data may end up being used inappropriately and giving rise to a

risk of usurpation or identity theft.

The proactive responsibility system implemented by the GDPR, focused on the

continuous management of the potential risks associated with the treatment, imposes on the

data controllers who analyze what data they process, for what purposes and what

types of treatments carried out, relating the potential risks to which they are

exposed and from there, decide what measures to take and apply to ensure their

compliance based

of the risks detected and assumed.

The impact assessment on the protection of personal data, EIPD, is the

tool that in the GDPR deals with the guarantee of compliance with this

treatment aspect.

In the text of the GDPR there is no definition for the term "assessment of

impact on data protection" or EIPD. The CEPD does develop the definition

of EIPD in the WP248 Guidelines as: “…a process designed to describe the

treatment, assess its necessity and proportionality, and help manage risks

for the rights and freedoms of natural persons derived from the processing of data

personal coughs by evaluating them and determining measures to address them.” According to

For this, the CEPD considers that the EIPD is a "process" and, therefore:

• Reducing the EIPD to a specific and isolated activity in time is incompatible with the

process concept that interprets the WP248 Guidelines.

• The EIPD must be documented, but the EIPD is more than the report that reflects

Your results.

• The EIPD must assess the risks “determining the measures to address them”. The

EIPD obliges the person in charge to act and has a greater dimension than a mere form-

isism embodied in a document on which minimal changes can be made

to adapt it to any treatment.

The EIPD is a process of analyzing a treatment that extends over time, over

throughout the entire life cycle of personal data processing, and that it has to be re-

continuously, “at least when there is a change in the risk that they represent

have treatment operations” (art.35.11 of the GDPR).

The defendant does not provide said document before the start of the procedure, and once

provided it is estimated that it does not meet the minimum requirements that it must contain , therefore

that he is charged with the infringement of article 35 of the GDPR, which states:

"1. When it is likely that a type of treatment, in particular if it uses new

technologies, by their nature, scope, context or purposes, entail a high risk for

the rights and freedoms of natural persons, the person responsible for the treatment carried out

An evaluation of the impact of the treatment operations will be carried out before the treatment.

compliance with the protection of personal data. A single evaluation may address a

series of similar processing operations involving similar high risks.

2. The person responsible for the treatment will seek the advice of the protection delegate.

data, if appointed, when conducting the impact assessment relating to the

Data Protection.

3. The impact assessment on data protection referred to in the

Paragraph 1 will be required in particular in case of:

a) systematic and exhaustive evaluation of personal aspects of natural persons

that is based on automated processing, such as profiling, and on

on the basis of which decisions are made that produce legal effects for natural persons

cases or that significantly affect them in a similar way;

b) large-scale processing of the special categories of data referred to

Article 9(1) or personal data relating to convictions and offenses

penalties referred to in article 10, or

c) large-scale systematic observation of a publicly accessible area.

4. The control authority will establish and publish a list of the types of operations

processing purposes that require a protection impact assessment

of data in accordance with paragraph 1. The supervisory authority shall communicate these

lists to the Committee referred to in article 68.

5. The control authority may also establish and publish the list of types

of treatment that do not require impact assessments related to the protection of

data. The supervisory authority will communicate these lists to the Committee.

6. Before adopting the lists referred to in paragraphs 4 and 5, the authority of

competent control will apply the consistency mechanism referred to in article

63 if those lists include processing activities that are related to the offer

of goods or services to interested parties or with the observation of the behavior of these

in several Member States, or processing activities that may substantially affect

especially to the free movement of personal data in the Union.

7. The evaluation must include at least:

a) a systematic description of the planned processing operations and the

purposes of the treatment, including, where appropriate, the legitimate interest pursued by the

responsible for the treatment;

b) an assessment of the necessity and proportionality of the processing operations;

lie with respect to its purpose;

c) an assessment of the risks to the rights and freedoms of the data subjects

referred to in paragraph 1, and

d) the measures planned to deal with the risks, including guarantees, measures of

security and mechanisms that guarantee the protection of personal data, and

show compliance with this Regulation, taking into account the rights

and legitimate interests of the data subjects and other affected persons.

8. Compliance with the approved codes of conduct referred to in article

40 by the corresponding managers or managers will be duly taken into

into account when assessing the impact of processing operations carried out by

said controllers or processors, in particular for the purposes of impact assessment

regarding data protection.

9. When appropriate, the controller will seek the opinion of the interested parties or their

representatives in relation to the planned treatment, without prejudice to the protection of

public or commercial interests or the security of processing operations.

10. When the treatment in accordance with article 6, paragraph 1, letters c) or e),

has its legal basis in Union law or in the law of the Member State

that applies to the data controller, such law regulates the specific operation

treatment or set of operations in question, and a

data protection impact assessment as part of an assessment

of general impact in the context of the adoption of said legal basis, paragraphs

1 to 7 shall not apply unless the Member States deem it necessary

proceed to said evaluation prior to treatment activities.

11. If necessary, the controller will examine whether the processing is in accordance with the

impact assessment relating to data protection, at least where there is a

change in risk posed by processing operations."

In development of paragraph 4, the Director of the AEPD approved a non-exhaustive list,

indicative of the types of treatment that require a relative impact assessment.

goes to data protection, indicating: "At the time of analyzing data processing,

data, it will be necessary to carry out a DPIA in most cases in which said

Treatment meets two or more criteria from the list below, except

that the treatment is on the list of treatments that do not require EIPD to the

referred to in article 35.5 of the GDPR.

"4. Treatments that imply the use of special categories of data to which

referred to in article 9.1 of the GDPR … or deduce information about the persons related to

comes up with special categories of data.

5. Processing that involves the use of biometric data for the purpose of identifying

charge uniquely to a natural person.”

In this case, it is the offer of services to those attending a Congress, established

creating an identification mechanism that enables contactless access based on

facial recognition with the taking of the template of your face that is managed in a pro-

computer program whose service is offered by a third party with which a

custom contract.

The obligation to carry out an impact assessment in this case is due to

that "uses new technologies, by their nature, scope, context or purposes, involves

a high risk for the rights and freedoms of natural persons”

In this case, the various risks that may arise must be analysed, including

its technology, within the framework of an increasingly intensive use of this type of data. His

use, interoperability and technological interconnection, is more than likely to interfere

with these fundamental rights and may give rise to questions about their

implantation.

The use of biometric data and, in particular, the RF entails greater risks for

the rights of the interested parties. It is essential that the use of these technologies be

done with due respect for the principles of legality, necessity, proportionality

and minimization of the data established in the GDPR. Although the use of these

technologies can be perceived as particularly effective, those responsible must, in

First, assess the impact on fundamental rights and freedoms and

consider less intrusive means to achieve your legitimate purpose of processing.

The “risk-based approach” is developed in the “Statement on the role of a

risk-based approach in data protection legal frameworks WP218" of GT 29, WP218, and

It is not a new concept in the framework of data protection.

Risk management for rights and liberties, aims to study the

impact and the probability of causing harm to people, at the individual or societal level,

as a result of the processing of personal data. On the contrary, management

of regulatory compliance risk is intended to provide the controller with a

tool to verify the degree of compliance with obligations and precepts

legally required in relation to a processing activity. Therefore,

prior to the risk management process and as a sine qua non condition for

undertake a processing activity, it is necessary to systematize the verification of

regulatory compliance throughout the entire treatment life cycle. The

complexity of the risk management process has to be adjusted, not to the size of the

entity, the availability of resources, its specialty or sector, but rather

possible impact of the processing activity on the interested parties and on the company itself

treatment difficulty.

As a potential source of risk, knowledge of the technologies that are intended to

use, as well as their associated risks, must be understood as an obligation

of the controller and part of their duty of care in relation to compliance with the

GDPR provisions.

Biometric processing presents, among others, the following risks, some of which

which are contemplated in Opinion 3/2012 on the evolution of technologies

biometrics of GT 29 of 04/27/2012:

-The definition of the size (amount of information) of the biometric template is a

crucial question. On the one hand, the size of the template must be large enough

to manage security (avoiding overlaps between the different data

biometrics, or identity substitutions), and on the other, it should not be too large

in order to avoid the risks of reconstruction of biometric data

-Risks involved in the use of biometric data for identification purposes in

large centralized databases, given the potential consequences

harmful to the people affected.

-It goes without saying that any loss of the qualities of integrity, confidentiality

and availability with respect to the databases would clearly be detrimental to

any future application based on the information contained in said databases

data, and would also cause irreparable damage to the data subjects. For example, if the

registered data of an authorized person will be associated with the identity of a

unauthorized person, the latter could access the services available to the

owner of the data, without having the right to do so. The result would be identity theft,

that (regardless of its detection) would make the system unreliable for future

applications and, consequently, would limit their freedom.

- The transfer of information contained in the database.

-It can create the illusion that identification through the face is always

correct, for this reason an analysis of the errors that can occur in

its use, performance evaluation meters, false acceptance rate-

probability that a biometric system will incorrectly identify an individual or

do not reject an individual who does not belong to the group, and rate of false rejection or false

negative: the correspondence between a person and his own template is not established.

Faced with decisions that legally affect a person, any decision that

is adopted based on this, such as in registration and time control systems, the deduction of fees for registration with the system, which should only be made safeguarding the rights and freedoms and the legitimate interests of the data subject, at least the right to obtain human intervention on the part of the controller, to express their point of view and challenge the decision.

-Linking: A large number of online services allow users to upload a image to link it to the user's profile. The RF can be used to link the profiles of different online services (via profile picture), but also between the online and offline world. It is not out of the question to take a photograph of a person on the street and determine their identity in real time looking at these public profile pictures. Third party services may also track profile photos and other publicly available photos to create large collections of images in order to associate a real world identity with

such images. This impact increases with the increasing deployment of these technologies. Each individual can appear in one or several biometric systems.

-Security measures must be adopted for data processing biometrics (storage, transmission, extraction of characteristics and comparison, etc.) and especially if the data controller transmits such data via Internet. Security measures could include, for example, the encryption of templates and protection of encryption keys apart from the access control and protection that makes it virtually impossible to

reconstruction of the original data from the templates. Additionally, use of
realistic or photo use masks to try to trick the system, always on
connection with the advances and the state of the art, taking into account that the
biometric systems that are more effective when it comes to recognizing a person are also
the most potentially vulnerable
Likewise, the working document on biometrics, adopted on 08/01/2003 by GT29,
is of the opinion that biometric systems relating to physical characteristics that do not allow
trace (for example the shape of the hand, but not fingerprints) or systems
biometrics relating to physical characteristics that leave a trace but do not depend on the
storage of data held by a person other than the interested party (in other
words, the data is not stored in the access control device or in a
central database) create fewer risks for the protection of rights and
fundamental freedoms of people (Biometric data can be distinguished
that are processed centrally from the biometric reference data that is
stored on a mobile device and the compliance process is performed on the card
and not on the sensor or when it is part of the mobile device).
-It is generally accepted that the risk of reusing biometric data obtained
from physical traces left by people inadvertently (for example: footprints
digital) for incompatible purposes is relatively low if the data is not
stored in centralized databases, but in the possession of the person and are
inaccessible to third parties. Centralized storage of biometric data
it also increases the risk of using biometric data as a key to
interconnect different databases, which could allow obtaining profiles
details of a person's habits both publicly and privately. Besides,
the question of the compatibility of the purposes leads us to the interoperability of
different systems that use biometrics. The standardization required

interoperability can lead to greater interconnection between databases.

-Role of the person in charge of treatment that is obliged to assist the person in charge to the

when carrying out the management, and that if you develop or supply a product as your

software, it must be incorporated into the treatment risk management process that

claims to be responsible. Option to audit the measures implemented by the

data controller

The claimant does not contemplate diverse and varied elements and scenarios that have been

indicated in this section in its risk assessment, and has provided an evaluation

of impact that was merely nominal, since it has not examined its aspects

substantive, neither assessed the risks nor the proportionality and necessity of the

implementation of the system, its impact on the rights and freedoms of the interested parties

and its guarantees.

In accordance with the available evidence, it is considered that the

The exposed individuals breach the provisions of article 35 of the GDPR.

V

The alleged infringement is typified in article 83.4.a) of the GDPR, which indicates:

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

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

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

overall annual total business of the previous financial year, opting for the one with the highest

amount:

a) The obligations of the controller and the person in charge under articles 8, 11, 25 to

39, 42 and 43;”

The LOPDGDD establishes for the purposes of prescription of the infringement, in its article 73.t):

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

They are considered serious and will prescribe after two years the infractions that suppose a vulnerability.

substantial portion of the articles mentioned therein and, in particular, the following:

t) The processing of personal data without having carried out the evaluation of the impact

of processing operations in the protection of personal data in the su-

posts in which it is enforceable.”

SAW

The determination of the sanction that should be imposed in the present case requires observing

vary the provisions of articles 83.1 and 2 of the GDPR, precepts that, respectively,

have the following:

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

pursuant to this Article for breaches of this Regulation indicated

in sections 4, 9 and 6 are effective in each individual case, proportionately

give and dissuasive.”

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

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

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

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

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

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

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

b) intentionality or negligence in the infraction;

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

settle the damages suffered by the interested parties;

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

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

articles 25 and 32;

e) any previous infringement committed by the 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 way in which the supervisory authority became aware of the infringement, in particular

determine whether the controller or processor notified the infringement and, if so, to what extent

gives;

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

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

same matter, compliance with said measures;

j)

notifications approved in accordance with article 42, and

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

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

mind, through infraction."

adherence to codes of conduct under Article 40 or to security mechanisms

Within this section, the LOPDGDD contemplates in its article 76, entitled "Sancio-

and corrective measures":

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

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

two in section 2 of said article.

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

may also be taken into account:

a) The continuing nature of the offence.

b) The link between the offender's activity and data processing;

personal coughs.

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

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

of the offence.

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

fraction, which cannot be attributed to the absorbing entity.

f) The affectation of the rights of minors.

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

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

alternative conflict resolution mechanisms, in those cases in which

there are controversies between those and any interested party.

3. It will be possible, complementary or alternatively, the adoption, when appropriate, of

the remaining corrective measures referred to in article 83.2 of the Regulation

(EU) 2016/679."

In accordance with the precepts transcribed, for the purpose of setting the amount of the sanction of fine to be imposed in the present case for the violation of article 35 of the GDPR, of the that the claimed entity is held responsible, are deemed concurrent as aggravating the following factors that reveal a greater illegality and/or guilt in his conduct:

-Article 83.2.a) of the GDPR: "a) the nature, seriousness and duration of the infringement, taking into account the nature, scope or purpose of the processing operation in question as well as the number of interested parties affected and the level of damage and damages they have suffered".

Data from a very high number of attendees, 20,000, were processed without considering the high level of risk in relation to the impact on their rights and freedoms that may exist for treatments based on facial recognition for access to the Congress.

- Article 83.2.b of the RGPD, "intentionality or negligence in the infringement". I don't know is aware that the entity has acted fraudulently, although the action reveals a serious lack of diligence in your conduct in taking action precise proactive measures in such a unique, differentiated and special regime applicable to the type of data that it deals with, without it being stated that the basic means have been put in place so that did not occur. In this regard, what was declared in the Judgment of the National Court of 10/17/2007 (rec. 63/2006) which, based on the fact that it is entities whose activity involves continuous data processing, indicates that "…the Supreme Court has been understanding that imprudence exists whenever disregards a legal duty of care, that is, when the offender does not behave with the due diligence. And in assessing the degree of diligence, consideration must be especially the professionalism or not of the subject, and there is no doubt that, in the case

now examined, when the appellant's activity is of constant and abundant

handling of personal data must insist on rigor and exquisite care

for complying with the legal provisions in this regard".

-Article 76.2.b) of the LOPDGDD "b) The link between the activity of the infringer and the

processing of personal data." The indisputable link between

activity of the defendant with the performance of data processing of a

staff, at least natural persons attending this type of massive event that

has been organizing for a long time (art 76.2.b of the GDPR).

In relation to the mitigations sought by the defendant:

-Estimating that the infringement was not continued, it only lasted from 03/22/2021 and ceased

four weeks after the end of the event, 07/29/2021.

The system was used every day and during the entire period of the Congress. The number

of daily attendees was presumably in the thousands, so even though

Outside of that space of time, its use was intensive and massive.

-Regarding collaboration by providing what is requested by the AEPD, it must be indicated that the

Article 5.2 of the GDPR, based on the principle of proactive responsibility, must be

interpreted broadly, in the sense that the data controller must

not only demonstrate that the data processing complies with the provisions of the same, in

In this case, before implementing biometric data, prepare an EIPD, and must

also prove that all the necessary conditions are met for said

treatment takes effect. Therefore, the collaboration and contribution of documents

to certify that the treatment conforms to the regulations is a minimum required, which

therefore, it must not produce any mitigation in case of infringement.

-Regarding the mitigating factor that the audience was familiar with the

technologies and can choose the RF option, the procedure does not start and resolve

for said use, but for not foreseeing the evaluation of the impact of the treatment.

In addition to the above, it adds that minors in the few cases that were

with an assistant, with them the F system was not used. This allusion to add it as

a mitigating factor in the sanction, it is still purely secondary and episodic, when

nothing has been specified about the minors in the procedure, their reference being

purely marginal, and not being attended to, being also analyzed, the validity

before processing the RF of a valid EIPD.

-Finally, not having committed previous infractions cannot serve as

extenuating

As a consequence with the elements that are available, the sanction is quantified in

200,000 euros.

VII

Article 58.2 of the GDPR provides the following: "Each control authority shall have

of all of the following corrective powers listed below:

[…]"

impose an administrative fine under Article 83, in addition to or instead of

Yo)

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

particular case;"

"d) order the controller or processor that the processing operations

compliance with the provisions of this Regulation, where appropriate, in accordance with

a certain manner and within a specified period;"

"The imposition of this measure is compatible with the sanction consisting of a fine

administration, according to the provisions of art. 83.2 of the GDPR."

Article 36.1 and 2 of the GDPR establishes:

"1. The person in charge shall consult the control authority before proceeding to the

processing when an impact assessment relating to data protection in

under Article 35 shows that the processing would entail a high risk if the

responsible does not take measures to mitigate it.

2. When the supervisory authority considers that the planned treatment referred to

paragraph 1 could infringe this Regulation, in particular where the

responsible has not sufficiently identified or mitigated the risk, the control authority

control must, within a period of eight weeks from the request for consultation,

advise in writing the person in charge, and where appropriate the person in charge, and may use

any of its powers mentioned in article 58. Said term may

extended by six weeks, depending on the complexity of the planned treatment. The

control authority will inform the person in charge and, where appropriate, the person in charge of such

extension within one month from receipt of the consultation request,

indicating the reasons for the delay. These terms may be suspended until the

supervisory authority has obtained the information requested for the purposes of the consultation."

In this case, only the required impact assessment has been assessed before

of data processing of the facial recognition system for access to MWC

of 2021, without questioning that of 2022.

Therefore, in accordance with the applicable legislation and assessed the criteria of

graduation of sanctions whose existence has been accredited,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE GSMA LIMITED, with NIF N4004237F, for a violation of the

article 35 of the GDPR, in accordance with article 83.4.a) of the GDPR, and for the purposes of

prescription, considered serious in article 73.t) of the LOPDGDD, a fine of

200,000 euros.

SECOND: NOTIFY this resolution to GSMA LIMITED and GSMC EVENT

PROJECT MANAGEMENT, S.L.

THIRD: Warn the penalized person that they must make the imposed sanction effective

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

art. 98.1.b) of Law 39/2015, of 1/10, on the Common Administrative Procedure of

Public Administrations (hereinafter LPACAP), within the voluntary payment term

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

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

17/12, by means of its entry, indicating the NIF of the sanctioned and the number of

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

IBAN: ES00-0000-0000-0000-0000-0000 (BIC/SWIFT Code:

restricted no.

CAIXESBBXXX), opened on behalf of the Spanish Data Protection Agency in

the banking entity CAIXABANK, S.A. Otherwise, it will proceed to its

collection in executive period.

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

between the 1st and 15th of each month, both inclusive, the term to make the payment

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

between the 16th and the last day of each month, both inclusive, the payment term
It will be until the 5th of the second following or immediately following business month.

In accordance with the provisions of article 50 of the LOPDGDD, this
Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process in accordance with art. 48.6 of the
LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the
Interested parties may optionally file an appeal for reversal before the
Director of the Spanish Agency for Data Protection within a period of one month from
count from the day following the notification of this resolution or directly
contentious-administrative appeal before the Contentious-administrative Chamber of the
National Court, in accordance with the provisions of article 25 and section 5 of
the fourth additional provision of Law 29/1998, of 07/13, regulating the
Contentious-administrative jurisdiction, within a period of two months from the
day following the notification of this act, as provided for in article 46.1 of the
referred Law.

Finally, it is noted that in accordance with the provisions of art. 90.3 a) of the LPACAP,
may provisionally suspend the firm resolution in administrative proceedings if the
The interested party expresses his intention to file a contentious-administrative appeal.
If this is the case, the interested party must formally communicate this fact through
writing addressed to the Spanish Data Protection Agency, presenting it through
of the Electronic Registry of the Agency [https://sedeagpd.gob.es/sede-electronica-
web/], or through any of the other registries provided for in art. 16.4 of the

mentioned LPCAP. You must also transfer to the Agency the documentation that accredits the effective filing of the contentious-administrative appeal. If the agency does not was aware of the filing of the contentious-administrative appeal in the period of two months from the day following the notification of this resolution, would terminate the injunction.

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-181022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es