 Procedure No.: PS/00225/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant) dated June 15, 2019

filed a claim with the Spanish Data Protection Agency. The

claim is directed against GLOVOAPP23, S.L. with NIF B66362906 (hereinafter, the

reclaimed). The grounds on which the claim is based are that in February 2018

requested the deletion of his account from the application, to which they replied to the email

email confirming receipt of your request. However, on 27

May 2019 received an email of an order placed with your account, the

which had not been done by the claimant. He contacted the company

through email and they replied “in a strange language, with characters

rare” requesting your credit card information, which you do not provide. Also

contacted via Twitter and was initially told that his email account was not

existed, that the order in question had been canceled and, subsequently, before his

request for access to the account to delete the bank details, they asked again for the

identification with your ID and credit card. When sending him the data, they replied that

they needed more credit card details, which he objected to. Request to be

eliminate their data "definitively from their Database, which they have already breached

one time".

Together with the claim, provide, among others, the following documentation:

-

Exchange of emails dated February 1, 2018 in which

the claimed, from the address support@glovohelp.***EMPRESA.1.com,

asks the claimant at his email address ***EMAIL.1 to

respond to that email to confirm the cancellation and tells you that "Remember that

Once processed, all your data will be deleted and you will not be able to return to

access the details of the balloons you have made". The claimant responds

with the confirmation of the cancellation and it is answered that "Your message nº (***ID.4) was

is managing to find the best possible solution".

-

- Email dated May 27, 2019, received in the account of

email from which the claimant requested the deletion of their

account, of a "Confirmed Order" written in Cyrillic alphabet letters, with

identification number "ID: KI17LG1HM".

Exchange of emails dated May 27, 2019 between the

claimant and liveops.comms@glovoapp.com in which he denounces that

made this request for someone else, but that the last four digits of your

credit card, which appear in the order mail, coincide with those of

your credit card and that you tried to connect to the application but it asked you

confirmation on the phone, which does not match your number. The claimed "for

ensure secure payment" asks the claimant to send you a copy of

your ID or passport and credit card, in which only the

holder's name and the first 6 digits and last 4 digits. the claimant

responds that he does not want to make any payment, that the last order did not

-

-

date 7 of

he did and that his identity was supplanted, that he cannot access the account

and that he is not going to send them his bank details because he sees a lack of security

important in the app and request that account be deleted.

Emails dated June 6, 2019 sent by

liveops.comms@glovoapp.com to the claimant indicating that the

account has been blocked for suspicious activities and they request a copy of

your ID or passport and the card in which only the name is seen

of the holder and the first 6 digits and last 4 digits in order to

verify identity to review account status. and mail

electronic strip

June 2019 Submitted By

liveops.comms@glovoapp.com to the claimant in which he is requested to

re-send the copy of your card because the data cannot be viewed.

6 first digits.

Exchange of messages on Twitter from May 27 to June 8

of 2019 in which the claimant states that an order has been made that he

has not applied, that he is worried because the last digits of the card

match yours, that you wanted to access your account and couldn't, and

that the phone to recover the password is not yours. The claimed in

At first, he answers that the email provided does not correspond to

no account and they ask for an order number that you had made in the

past. The claimant provides them with the order number #GJPYLGSVC of

dated 01/06/2018 and the respondent replies that he is aware that the request is not

requested has been canceled without costs and that you will receive the amount charged

incorrectly. The complainant insists that he wishes to remove his data from the

application, for which you want to access it. To do this, the respondent

asks you to perform "a verification that we have sent to your email". The

claimant reproduces the mail in which they request a copy of the DNI and a copy of

the credit card associated with the account that shows your name and the 6

first digits and last 4 digits. The claimant indicates that he sent the photo,

but the claimed insists that the attached images cannot be

display the first six digits of the card and that they need that

information “in order to enable your profile”. The claimant refuses to provide

this data due to distrust in the security of the application, since

in February he had asked to delete the account and they had told him that

they would, but months later you get a message that an order was placed

from the account you had requested to delete. He states that he only wanted

access the application to remove your credit card number and that

you want to delete that account, along with all your personal data. Finally,

the respondent insists that he needs to verify his identity “to proceed with the

refund of the amount paid and then we can cancel the account”. The

Claimant answers that they had first told him that there was no account

with your email, after an order has been blocked with your account (the one that

had said it did not exist), they later told him that the money had been

returned and now they asked for more information to return the amount that was already

was returned, that it was clear that something was wrong or that the

claimed and that he was going to file a complaint with this Agency.

SECOND: Upon receipt of the claim, the Subdirectorate General for

Data Inspection on 08/12/2019 transferred the claimant to the claim

submitted for analysis and communication to the claimant of the decision adopted

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

regard. Likewise, it was required that within a month he send to the

Agency certain information:

The decision made regarding this claim.

In the event of exercising the rights regulated in articles 15 to 22

of the RGPD, accreditation of the response provided to the claimant.

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

claim.

Report on the measures adopted to prevent the occurrence of

similar incidents, dates of implementation and controls carried out to

check its effectiveness.

Any other that you consider relevant.

On 09/10/2019, the response of the respondent with the number of

entry record 042819/2019, in which the following is provided, among others

information:

-

-

-

-

-

-

Regarding the decision adopted regarding this claim: first

First, the respondent states that “the claimant, having consented to the

Terms of Use of the platform and having consented to the terms of our

Privacy Policy, you accept that the obligation belongs to the user

to demonstrate that you exercised your right to process your personal data

in the forms established in our Privacy Policy”. second

Firstly, it affirms that the defendant, "in his capacity as Responsible for the

treatment, adopted at the time the necessary measures to proceed to

the deletion of your data, however, article 17.3. e) of the RGPD allows

substantiate the possibility of retaining personal data despite the fact that

the user has withdrawn their consent to treat them, as long as

said conservation is based on the need to defend the legal interests

and administrative of the company responsible for the treatment”. And that

right of suppression is not an automatic right, but must be fulfilled

one of the previously detailed requirements” in art. 17.3 and that “art. 17.

3.e) allows the conservation of the data, among other cases, as long as

when necessary for the formulation, exercise or defense of

claims”, such as the one in this case. Third, it indicates that the

claimed acted with due diligence since the claimant received a

response to your email confirming receipt

of your request, which shows that the request of the

claimant and keeps you informed about the status of your application. In fourth

Firstly, it affirms that the defendant "has adopted the security measures

necessary and appropriate to the existing level of risk to avoid breaches,

leaks and mistreatment of personal data in its treatment system” and that

when a user of your mobile application is the victim of a hack of their

email account, "it cannot be considered that such access does not

authorized is due to the presumed deficiencies of the security system of

an application" like that of the respondent, which "has been recognized and accepted

by the user himself, when downloading the mobile application" and having

accepted its Terms and Conditions and its Privacy Policy. Finally,

the respondent indicates that, in addition to canceling the order supposedly

fraudulent and not billing the claimant, to reactivate your user in the

application is required to pass certain security measures, such as facilitating

personal and bank details, which the claimant has decided not to provide.

-

-

-

Regarding the exercise of the rights regulated in articles 15 to 22 of the

RGPD: the claimed party affirms that when requesting personal data from the claimant

such as your ID or bank details to be able to access your account again,

it can be verified that the RGPD has been correctly complied with,

"by freezing all your personal information in our databases, a

was once requested by the claimant. Such freezing does not mean deletion

total, since according to art 17.3.e) this could produce a situation

of inequality" between the claimed and the claimant.

Regarding the causes of the incident: the respondent points out as possible

external cause unauthorized access to the user's email,

victim of a hack.

Regarding the measures adopted to avoid similar incidents: the

claimed lists the freezing and pseudonymization of the data of the

claimant, in accordance with the aforementioned art. 17.3.e); the cancellation of the order

allegedly fraudulent, despite the fact that this could be due to a possible

hacking not attributable to the claimed; and that they proceeded to signal and block the

complete profile of the user, in order to avoid possible fraud that could

affect you.

On 09/26/2019, in accordance with article 65 of the LOPDGDD, the Director of the

Spanish Agency for Data Protection agreed to admit the claim for processing

filed by the claimant against the respondent.

THIRD: In view of the facts outlined above, the Subdirectorate General

of Data Inspection proceeded to carry out preliminary actions of

investigation to clarify the facts in question, by virtue of the

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

Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter

RGPD) and in accordance with the provisions of Title VII, Chapter I, Section

second, of Organic Law 3/2018, of December 5, on Data Protection

Personal and guarantee of digital rights (hereinafter, LOPDGDD).

As a result of the research actions carried out, it is found that the

responsible for the treatment is the claimed.

Likewise, on February 12 and March 4, 2020, an inspection was carried out

face-to-face at the defendant's headquarters, in which the following information was obtained, among others:

information, as can be deduced from the report of previous actions dated

08/13/2020:

-

-

The respondent stated that, at the end of 2018, a measure of

security in its application that consisted in that, whenever a user

authenticate from a new device, a verification code is sent to the

mobile phone that was entered during the registration process. This process

was already used during the registration process to verify that the number of

phone entered was in the possession of the user.

The respondent stated that, after the completion of each order, it is verified

automatically if the operation matches any pattern of attempted

fraud and, if so, an alert appears so that an employee of the

investigated block the account manually and someone from the department of

fraud request more information from the user via email with the

-

-

-

-

-

-

purpose of lifting the blocking of the account. While the lockdown lasts

account, if the user tries to access his account, a message is displayed

Notice telling you to contact customer service; this message is

see in the screenshot example provided during the inspection.

The respondent stated that the data of the accounts whose users have

requested deletion or that have been blocked due to suspected fraud

are kept for the periods established for accounting reasons,

operational, fiscal and prescription of crimes and infractions of the

money laundering prevention regulations.

The respondent stated that, of the credit cards, they are only stored in

its information systems the first 6 and the last four digits; the

The rest of the credit card data has only been known by the

user and their payment gateway service provider.

The respondent stated that the claimant requested the cancellation of his account

user but did not confirm that cancellation; and that the account was blocked when

the respondent was aware that this account could be subject to

fraud, and subsequently the user account was deleted.

The user account with which the order was supposedly placed on the 27th of

May 2019 has the date of creation in the information systems

of the claimed on June 1, 2018, and as erasure date the 10 of

September 2019. This follows the screenshots taken

during the inspection in the database and on the platform of

administration of the investigated on the order KI17LG1HM and the data of the

customer ***ID.4, associated with that order.

At the time of the inspection, the customer data ***ID.4,

associated with the order placed on May 27, 2019, were marked

as “FRAUD DELETED” and had been pseudonymized, without appearing the

name or surname of the client in the administration platform, which

is clear from the screenshot of the customer data ***ID.4 in the

claimed administration platform.

In the document filed on behalf of the respondent, dated in

the AEPD on July 17, 2020 and entry registration number 025445/2020,

the following is declared: That after the deletion of the data, to demonstrate the

traceability of the protocol carried out, a new profile was created ad hoc without

personal information; for this reason, the date of creation provided coincides with

the date of account deletion.

FOURTH: On September 1, 2020, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimant, with

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

Common Administrative Procedure of Public Administrations (hereinafter,

LPACAP), for the alleged infringement of Article 6.1 of the RGPD, typified in Article

83.5.a) of the GDPR.

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

allegations dated September 30, 2020 in which, in summary, it stated

that “the events that occurred in relation to the account of the complaining user coincide

fully with the usual behavior pattern of cybercriminals who use

data traded on the black market in Eastern European countries such as

Ukraine to impersonate the identity of its victims and make fraudulent purchases.

In this specific case, we will see that the cyberattack is carried out from Ukraine and that

takes advantage of the negligent action of the claimant, by repeatedly using the same

key in different services that were affected by a security breach that

exposed his credentials.

After the different hypotheses analyzed in the investigation, my client has arrived

to the conclusion that these credentials were used by the claimant and

subsequently by the attacker in successive Glovo accounts.

“The website haveibeenpwned.com offers a free service that allows anyone to

user to check if his email address appears on these lists, and therefore

So, if your keys have been compromised and you need to change them immediately. Yes

we introduce the address ***EMAIL.1 in this database, it is verified that the

The claimant's credentials have been exposed in five security breaches and

two attempts or indications of attack”.

“This means that the email address and passwords of the

claimant have been exposed in five security breaches or disclosures of

data from different servers:

● Three security breaches prior to opening the Glovo account.

● A list of exposed data discovered prior to opening the account

in Glovo.

● A list of rich data discovered after the opening of the

account in Glovo, but with data that was older. We attach

as DOCUMENT ONE the report on these security breaches”.

The respondent also alleges that “The investigation also showed that the

The claimant had another Glovo account opened with the address ***EMAIL.2, address

delivery and credit card (matching initial and final digits). Using the

same resource, it is verified that this direction was exposed in nine breaches of

security".

“Cyber attacks based on lists of credentials acquired on the black market

exploit the negligence of users who use the same passwords in

the different online services they hire.

This would justify the fact that the claimant's credentials appeared on lists

enriched. Rich lists include data that has been verified and that

have been completed with the contributions of other cybercriminals who have

successfully exploited.

The end result is that the data of the claimant initially exposed in these

lists were limited to the email address and password, and, in the

latest versions of 2019 the claimant data had been enriched with

much more data, including:

1. Geographic location

2. Employment data

3. Phone numbers

4. Profiles on social networks

5. Credit cards”

“This makes it an exponent of scant diligence in the management and custody of its

credentials, as your history of keys exposed in security breaches is

starts in 2008 and runs through 2019, and the success of identity theft confirms

that during all this time the claimant has not changed the access codes

repeatedly engaged.

In the Terms and Conditions that regulate the service, available at

https://glovoapp.com/es/legal/terms, Glovo warns users of its

responsibility with respect to the choice of your passwords and when using the app of

Glovo the user expressly accepts these obligations:

“Clause 17. - Users are fully responsible for the access and correct

use of your profile and other contents of the Platform subject to legality

in force, whether national or international of the Country from which you use the Platform,

as well as the principles of good faith, morality, good customs and public order.

And specifically, it acquires the commitment to diligently observe these

General Conditions of Use.

Users are responsible for correctly consigning usernames and

individual, non-transferable and sufficiently complex passwords, as well as not

use the same username and password as on other platforms, all with

the purpose of protecting your account from fraudulent use by third parties unrelated to the

platform. (...)”

The defendant in his allegations raises four possible lines of investigation:

“The change of the CRM application destined to collect all the actions and

customer transactions prevents my client from having the logs with the details

of the operations carried out in 2018, so the investigation has focused on

verify or refute the four working hypotheses that we will develop in the following

points, showing that Glovo's performance has been diligent in the four

scenarios.

1. First hypothesis. - The cyber attacker used the credentials of the claimant,

unlocked and restored the old account.

2. Second hypothesis. - The claimant never verified his mobile phone number and the

double factor authentication was left unactivated. It is possible that an account

inactive for a few months (dormant account), go into a sleep mode

semilock and do not react to the delete command.

3. Third hypothesis. - The cyber attacker created a new account using the address

e-mail and credit card data of the claimant, obtained in

the black market

4. Fourth hypothesis. - The claimant opened a new account after deletion

from the previous one."

Regarding the first hypothesis (that the cyber attacker used the credentials of the

claimant and restored the old account), the respondent lists in his pleadings

a series of requirements that should have been met and concludes that the respondent made the

deletion and blocking of the claimant's data correctly and that he communicated

suppression to the claimant, for which he provides as DOCUMENT 2 the capture of the

screen extracted from the backup, in which this confirmation appears.

In this Document 2, a table is attached in which you can see, among other things, the

Next information:

go

subject

submitter

comment

***ID.4

Elimination

account

***ID.4

Elimination

account

***ID.4

Elimination

account

***ID.4

Elimination

account

C/ Jorge Juan, 6

28001 – Madrid

{'id':

116472211014,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

472211014.json',

'name': 'A.A.A.',

'e-mail':

***EMAIL.1',

'created_at':

'2018-01-

{'id':

116472211014,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

472211014.json',

'name': 'A.A.A.',

'e-mail':

***EMAIL.1',

'created_at':

'2018-01-

{'id':

116472211014,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

472211014.json',

'name': 'A.A.A.',

'e-mail':

***EMAIL.1',

'created_at':

{'id':

116472211014,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

472211014.json',

message

created at

2018-02-

01T19:39:3

4,000z

2018-02-

01T19:40:2

8,000z

Hello, I have been searching so much in the

application how on the website, and I have not

found nowhere way to

delete the account. I understand that this

It should be possible in a simple way

(although it is hidden), and if it cannot be

from the App that was from the page

Web. can you tell me how should i

proceed about it?

Hi A.A.A! goodbyes are always

tough, we don't want you to go! :(,

although we would like to know the reason why

which you have decided to leave, we care about you

opinion! If you have already thought it through and

want to delete your account, reply to this

email confirming the cancellation and we will manage

your request as soon as possible.

Remember that once processed, all your

data will be deleted and you will not be able to

access the details of

I confirm the deletion, thanks Greetings

On Feb 1, 2018, at 8:40 p.m., Glovo

<support@glovohelp.***COMPANY.1.com>

wrote:

2018-02-

01T19:44:1

8,000z

2018-02-

01T19:49:2

2,000z

solved in ***ID.4

I want to delete my Glovo account

2018-02-

01T19:45:3

0.000Z

Send

https://glovoapp.com/en/contact

since:

Hi A.A.A! goodbyes are always

tough, we don't want you to go! :(,

although we would like to know the reason why

which you have decided to leave, we care about you

opinion! If you have already thought it through and

want to delete your account, reply to this

email confirming the cancellation and we will manage

your request as soon as possible.

2018-02-

01T19:47:1

8,000z

2018-02-

01T19:47:5

6,000z

2018-02-

01T19:48:4

3,000z

On Feb 1, 2018, at 8:47 p.m., Glovo

<support@glovohelp.***COMPANY.1.com>

wrote:

Hi A.A.A! There is no going back :(

We confirm that we have deleted your

user account of our database

data. As we told you, not anymore

you will not be able to access your profile or the details of

your previous orders. The drop in shipping

from the newsletter to your email

will be effective in approximately 48

working hours

I want to delete my account, linked through

From Facebook,

2018-02-

01T19:46:2

3,000z

Thank you

a greeting

---

since:

Send

https://glovoapp.com/en/contact

Hi A.A.A! goodbyes are always

tough, we don't want you to go! :(,

although we would like to know the reason why

which you have decided to leave, we care about you

opinion! If you have already thought it through and

2018-02-

01T19:48:1

0.000Z

www.aepd.es

sedeagpd.gob.es

'name': 'A.A.A.',

'e-mail':

***EMAIL.1',

'created_at':

360237355414,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/360

237355414.json',

'name': 'A.A.A.',

'e-mail':

{'id':

360237355414,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/360

237355414.json',

'name': 'A.A.A.',

'e-mail':

'***EMAIL.3

360237355414,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/360

237355414.json',

'name': 'A.A.A.',

'e-mail':

{'id':

360237355414,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/360

237355414.json',

'name': 'A.A.A.',

'e-mail':

'***EMAIL.3

{'id':

116018503873,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

018503873.json',

'A.A.A.,

'yam':

'e-mail':

'***EMAIL.2

{'id':

116018503873,

'url':

'https://glovoservi

ce.*** COMPANY.

1511051 Disposal

account

1511051 Disposal

account

1511051 Disposal

account

1511051 Disposal

account

***ID.5

Elimination

account

***ID.5

Elimination

account

C/ Jorge Juan, 6

28001 – Madrid

10/37

2018-02-

01T19:48:4

8,000z

2018-02-

01T19:52:5

4,000z

***ID.5

Elimination

account

***ID.5

Elimination

account

1.com/

api/v2/users/116

018503873.json',

'A.A.A.',

'yam':

'e-mail':

'***EMAIL.2

{'id':

116018503873,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

018503873.json',

'name': 'A.A.A.',

'e-mail':

'***EMAIL.2

{'id':

116018503873,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

018503873.json',

'A.A.A',

'yam':

'e-mail':

'***EMAIL.2

want to delete your account, reply to this

email confirming the cancellation and we will manage

your request as soon as possible.

Remember that once processed, all your

data will be deleted and you will not be able to

access the details of

I confirm the deletion of the account, a

greeting

On Feb 1, 2018, at 8:48 p.m., Glovo

<support@glovohelp.***COMPANY.1.com>

wrote:

Hi A.A.A!

There is no turning back :(We confirm

that we have deleted your user account

from our database.

As we mentioned, you will no longer be able to

access your profile or the details of your

previous orders.

The cancellation of the sending of the newsletter to your

email will be effective in

approximately 48 business hours.

If you have any other questions at

respect, do not hesitate to contact us

replying to this same email.

The claimed party indicates that in order to have made the fraudulent order, the cybercriminal

you should have gotten admin permissions and done all the steps

described and having circumvented all the obstacles established to prevent it.

It also points out that it would be absolutely disproportionate to mount such an attack

powerful to make a tiny order.

For all these reasons, the respondent concludes that this first hypothesis must be rejected.

The respondent also points out the possibility that the confusion generated by the

duplication of accounts of the claimant and the exercise of the right of deletion limited to

one of them made the other remain operational and that was the one that the attacker

used to impersonate the claimant's identity.

Regarding the second hypothesis (the claimant never verified his telephone number
mobile and the double authentication factor was left unactivated. An account may
to be inactive for a few months (dormant account), go into a sleep mode
semi-blocking and does not react to the deletion order), the respondent alleges that "a
account not verified and without the double factor activated matches a pattern of attempt of
fraud and therefore the account is blocked. This lock would be different from the post lock
deletion, since in fraud attempts the blocked data remains in the database
main data because they must be consulted by the anti-fraud team to prevent
new fraud attempts.

However, this hypothesis does not fit with the fact that my client verified and
confirmed in February 2018 that the account had been successfully deleted."

"In any case, the blocking derived from a suspicion of fraud, justifies that the
data are kept in the main database, since they serve to verify new
fraud attempts coming from the same email account, the same
mobile or the same final figures of the credit card.

My client understands that the maintenance of data suspected of having
participated in a fraud attempt is a correct and necessary purpose to protect
to the client itself, which would justify its conservation in the main database after the
claimant's deletion request.

Regarding the third hypothesis (the cyber attacker created a new account using the

email address and credit card details of the claimant,

obtained on the black market), the respondent alleges that "The AEPD found, in the

course of the inspection at Glovo, and considers it a proven fact that the

Fraudulent order was made with an account that had been created on June 1,

2018. This is repeated several times in the agreement to start the sanctioning procedure

and in the records of the inspection.

This information is very important, because it shows that the account with which the

fraudulent order was not the same one that the claimant created. IT'S AN ACCOUNT

DIFFERENT.

The first account had the ID ***ID.1 and the second had the ID ***ID.3.

In addition, the first account used a MASTERCARD card and the second a card

VISA.

Let us remember that the proven facts begin in February 2018, when the

complainant requests the deletion of his account and the deletion of his data.

However, the checks carried out by the AEPD show that the account

used to place the fraudulent order was created FOUR MONTHS LATER

that the claimant requested the cancellation of his account and Glovo proceeded to

delete and block the data.

We understand that it was the cybercriminal who opened that account in June 2018 with

the data that it had obtained in the lists of e-mail addresses that were

they sell on the internet and on the black market.

This would certify that the deletion of the account and the blocking of the data was carried out

correctly, otherwise the cybercriminal would not have been able to use the

same email address.

The respondent indicates that, for this hypothesis to be feasible, there should have been

met the following requirements:

The respondent also alleges that it is notorious and widely known that, in the

deep internet black market, credit card data can be acquired

that have been exposed and that lists of accounts can be purchased with credit cards

credit not canceled after a security breach. And that the defendant defends that the

cyber attacker obtained the credit card data associated with the address of

claimant's mail on one of these lists.

To do this, it highlights two facts:

1. The claimant suffered a security breach in their Dropbox account, where

could keep your credit card details.

2. The claimant's details were on the enriched list that was discovered in

2019, but contained data from a higher age, which had been

enriched with contributions from other cybercriminals.

The defendant points out that Ukraine is also a country historically related to

phishing, so the ease of accessing credit card data is very

higher than that of other countries. And that, for all these reasons, he considers that the most probable option

It is possible that the cybercriminal used the claimant's credit card details

to place the fraudulent order, since the other options are much less

probable.

The respondent also points out that the charge related to the fraudulent order never reached

be made, since it was Glovo that detected a suspicious pattern and blocked the payment,

Therefore, no damage was caused to the claimant at any time.

Finally, the respondent indicates that, according to the evidence contained in the procedure, obtained during the inspection at the Glovo offices, and provided by the claimant and the respondent, the chronology of the events is as follows:

And it alleges that “This chronology fits perfectly with the proven facts and demonstrates that my client acted diligently and without violating the regulations of Data Protection.

The simple possibility that the events occurred in this way and not As the Agency maintains, but does not prove, it allows my client to benefit from the principle of presumption of administrative innocence and adopts as a hypothesis more plausible that relating to the creation of a new account by the attacker, which in at no time has it been contradicted by the Agency.”

Regarding the fourth hypothesis (the claimant opened a new account after the deletion of the previous one), the respondent indicates that this hypothesis would not be unreasonable, since, in addition to the Glovo ***EMAIL.1 account, the claimant had the account ***EMAIL.2, of which he had forgotten its existence, or at least only exercised the right of suppression in relation to one of them.

"For this reason, and despite the fact that the system logs do not keep the data from June 2018 to check the IP address from which the opening of this new account, it is perfectly feasible that the claimant opened a new account on June 1, 2018 and then forget that he had opened it.

This hypothesis would fully fit with the initial deletion of the data and the subsequent

identity theft by the cybercriminal, since the data of the

second account opened by the claimant would not have been deleted.

Remember that the IDs of the two accounts were different and the credit cards

also.

The chronology of events relating to this hypothesis would be as follows:

This timeline also fits the proven facts and shows that my

represented acted diligently and without infringing data protection regulations.

Also in this hypothesis, the simple possibility that the events occurred

in this way and not as the Agency maintains, but does not credit, allows my

represented to benefit from the principle of presumption of administrative innocence and adopts

The most plausible hypothesis is the one related to the creation of a new account by

of the claimant, which has never been contradicted by the Agency".

The respondent also alleges that he has carried out the following improvement actions since

2018:

"1. Change of the CRM software with which the relationship with customers is managed,

passed from the application ***COMPANY.1 to ***COMPANY.2.

2. Maintenance and improvement of the platform that prevents fraud and blocking actions.

quea attempts that respond to a suspicious pattern.

3. Maintenance and improvement of the double authentication factor, eliminating the risk related

tive to inactive accounts whose mobile phone was not verified and the double factor was not

was activated.

4. Pseudonymization of data blocked on suspicion of fraud.

5. Application of verification measures for users with two accounts as a result of the

case ***CASE.1, which also reached the AEPD.”

The respondent also points out that "in each of the working hypotheses considered

Glovo acted in accordance with the law and that in no case did it maintain the data of the claim.

remain accessible to persons other than those authorized to access the data

locked in the datawarehouse.

Different firms of recognized prestige have issued, prior to the closing of

each of the funding rounds, status reports on compliance

company regulations (Due Diligence). My client has punctually complied

the recommendations contained in said reports in order to ensure the protection

tion of the rights and freedoms of the interested parties.

In none of these reports has it been indicated that Glovo has measures of

insufficient security in relation to the user authentication process”.

Finally, the respondent indicates that "he considers the application of

of the aggravating criteria that have been taken into account at the time of graduating the

sanction.

1. In relation to the continuing nature of the infringement, my client has accredited-

that the chronology of the events maintained by the AEPD does not correspond to the

reality and that no infringement has occurred.

2. In relation to the number of users, this is wrong, since the figure is very

lower and for the purposes of this procedure should be taken into account only the

active accounts. If it were true that my client processes the data of more than 7 million

active customers, it would be a great success to have had a single incident of these

characteristics, since by simple statistical probability, human errors or

computer systems show much higher incident figures".

And that "he understands that it has been duly demonstrated that Glovo has acted in

at all times in good faith, using your best commitment, and never compromising

jeopardize the rights and freedoms of the interested parties. There is, therefore, no clear "intention"

tionality" in failing to comply with current regulations since, my client made all

the necessary and due actions for compliance with the regulations and has adjusted

prudently his acting to the law".

Then request:

- That the allegations to the agreement to open proceedings be considered filed.

sanctioning procedure and Procedure PS/00225/2020 is archived.

- That the aggravating criteria mentioned in said agreement are not applied.

- That the initially proposed penalty be reduced by 25% for having acted

company at all times in good faith, without having jeopardized the rights and liberties

liberties of the interested parties.

- That a reduction of 25% be applied for prompt payment, being applied on an

both reductions are mulative.

SIXTH: On February 12, 2021, the instructor of the procedure agreed to the

opening of a period of practice tests, considering incorporated the

claim filed by the claimant and his documentation, the documents

obtained and generated by the Inspection Services before the claimed party, the Report

of previous inspection actions that are part of file E/10306/2019,

as well as the allegations to the initiation agreement PS/00225/2020 presented by the

claimed and the documentation that accompanies them.

On February 15, 2021, the AEPD has required the person claimed so that in the

Within ten business days, submit the following information:

1) Screenshots with the search procedure that allows identifying what

the Glovo user account with ID ***ID.1 was associated with the email address

electronic ***EMAIL.1. Detailed description of the search procedure

done at this point.

2) Screenshots with the search procedure that allows identifying the

creation date of the Glovo user account with ID ***ID.1. Description

detailed description of the search procedure carried out at this point.

3) Screenshots with the search procedure that allows identifying the

blocking date of the Glovo user account with ID ***ID.1. Description

detailed description of the search procedure carried out at this point.

4) Screenshots with the search procedure that allows identifying the

date of deletion of the Glovo user account with ID ***ID.1. Description

detailed description of the search procedure carried out at this point.

On March 10, 2021, the respondent filed a response brief before this

Agency, in which it stated that "based on the information contained in our

information systems, the Glovo user account associated with the address of

email ***EMAIL.1 does not correspond to the ID ***ID.1, but to the ID ***ID.4".

And that "all information provided to this Agency by this

written corresponds to the Glovo user account associated with the email address

email ***EMAIL.1 identified in the information systems of my client

with the ID ***ID.4".

Next, the respondent provides the required information, but with respect to the

Glovo ID account ***ID.4.

On March 18, 2021, the AEPD has required the person claimed so that in the

Within ten business days, submit the following information:

1) Screenshots with the search procedure that allows identifying the ID

of the Glovo user account of the query id***ID.4, associated with the address of

email ***EMAIL.1. Detailed description of the search procedure

done at this point.

2) Screenshots with the search procedure that allows identifying the

creation date of the Glovo user account of the query id***ID.4, associated

to the email address ***EMAIL.1. Detailed description of the

search procedure performed at this point.

3) Screenshots with the search procedure that allows identifying the

blocking date of the Glovo user account of the query id***ID.4, associated with

the email address ***EMAIL.1. Detailed description of the procedure

search performed at this point.

4) Screenshots with the search procedure that allows identifying the

date of deletion of the Glovo user account from the query id***ID.4, associated

to the email address ***EMAIL.1. Detailed description of the

search procedure performed at this point.

All of this based on the fact that in his brief of allegations dated 09/30/2020, number of entry record O00007128e2000003988, GLOVOAPP23, SL alleges on page 5 that: “The investigation carried out by my client concludes that Glovo carried out the deletion and blocking of the claimant's data correctly and that he communicated deletion to the claimant. The screenshot is provided as DOCUMENT 2 extracted from the backup, in which this confirmation appears”. And that in the Document 2 that accompanies these allegations, in the first four rows it contains an id***ID.4 query and the timeline of the query, showing that the query id***ID.4 was associated with the email address ***EMAIL.1.

On April 12, 2021, the respondent filed a response brief before this Agency, in which it stated that “the specific additional information required by this Agency regarding specifically the query with ID***ID.4 associated with the email address ***EMAIL.1 is not stored in the database data of my represented”.

It points out that “the query with ID ***ID.4 is a reference number created by internal and organizational effects by the previous customer service provider client (*** COMPANY.1) that collaborated with Glovoapp23, S.L. in the moment in which the user ***EMAIL.1 made the aforementioned query on February 1, 2018, as As can be deduced from DOCUMENT No. 2 provided by this party in its brief of dated September 30, 2020. Each reference number was intended to identify the queries or incidents sent by the users of my represented and that should be attended by that provider.

The complainant indicates that "a change was made to the CRM software with which managed the relationship with its clients in order to increase security and

reliability of data deletion and blocking processes. In this sense, as

this party indicated in the FOURTH allegation of the aforementioned pleadings brief dated

September 30, 2020, said CRM change prevented you from having the additional data

about the query with ID ***ID.4 dated February 1, 2018, so this

party cannot provide additional data beyond the information on this

query that this party has already presented in the framework of this procedure.

My client wishes to emphasize that this is due to the fact that the previous supplier of the

customer service (*** COMPANY.1) had defined a period of

conservation of the data of the users that it treated in the name and on behalf of its

customers (in this case, Glovoapp23, S.L.) within a maximum period of 90 days from

from the end of the contractual relationship, a period that has already elapsed".

The respondent also recalls that "he has already provided this Agency with the information

had about the query with ID ***ID.4 made by the user ***EMAIL.1, such as

It is stated in his pleadings brief dated September 30, 2020 and that

understands this information as complete as it is made up of, among other elements:

reference ID number, contact method, query creation date, type of

query, subject, description and content of the query, conversations held

between the customer service agent and the user, timeline of the

consultation and identification of the user ***EMAIL.1 as the user who made the

query".

And it states that "it does not have in its databases additional information to the

regarding the query with ID ***ID.4 made by the user ***EMAIL.1 that already

provided both in the inspection process initiated by this Agency in the month of

February 2020, as in the different writings presented to this Agency

including the one dated September 30, 2020".

SEVENTH: On 05/21/2021, the requested resolution is notified to the respondent

in which it is proposed that, by the Director of the Spanish Agency for the Protection of

Data proceed to the FILE of this procedure against the entity, GLO-

VOAPP23, S.L. with CIF: B66362906, for alleged violation of article 6.1 of the

GDPR.

EIGHTH: After notification of the resolution proposal, the respondent has not pre-

laid down any type of allegation to the motion for a resolution.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

FACTS

FIRST: on June 15, 2019, the AEPD received a document in which the

The claimant stated that in February 2018 he requested the deletion of his account

the claimed application, to which they replied to the email with the

confirmation of receipt of your request. However, on May 27, 2019

received an email of an order placed with your account, which had not

been made by him. contacted the company via email

email and they replied "in a strange language, with strange characters" requesting

your credit card details, which you do not provide them. He also contacted through

Twitter and initially told him that his email account did not exist, that the order in

question had been canceled and, later, in response to his request for access to the

account to delete the bank data, they asked again for identification with your DNI

and credit card. When sending the data, they replied that they needed more data

of his credit card, to which he objected. Request that your data be deleted

"Definitely from their Database, which they have already breached once."

SECOND: the claimant has provided:

-

Exchange of emails dated February 1, 2018 in which

the claimed, from the address support@glovohelp.***EMPRESA.1.com,

asks the claimant at his email address ***EMAIL.1 to

respond to that email to confirm the cancellation and tells you that "Remember that

Once processed, all your data will be deleted and you will not be able to return to

access the details of the balloons you have made". The claimant responds

with the confirmation of the cancellation and it is answered that "Your message nº (***ID.4) was

is managing to find the best possible solution".

- Email dated May 27, 2019, received in the account of

email from which the claimant requested the deletion of their

account, of a "Confirmed Order" written in Cyrillic alphabet letters, with

identification number "ID: KI17LG1HM".

Exchange of emails dated May 27, 2019 between the

claimant and liveops.comms@glovoapp.com in which he denounces that

-

-

date 7 of

made this request for someone else, but that the last four digits of your

credit card, which appear in the order mail, coincide with those of

your credit card and that you tried to connect to the application but it asked you

confirmation on the phone, which does not match your number. The claimed “for

ensure secure payment” asks the claimant to send you a copy of

your ID or passport and credit card, in which only the

holder's name and the first 6 digits and last 4 digits. the claimant

responds that he does not want to make any payment, that the last order did not

he did and that his identity was supplanted, that he cannot access the account

and that he is not going to send them his bank details because he sees a lack of security

important in the app and request that account be deleted.

Emails dated June 6, 2019 sent by

liveops.comms@glovoapp.com to the claimant indicating that the

account has been blocked for suspicious activities and they request a copy of

your ID or passport and the card in which only the name is seen

of the holder and the first 6 digits and last 4 digits in order to

verify identity to review account status. and mail

electronic strip

June 2019 Submitted By

liveops.comms@glovoapp.com to the claimant in which he is requested to

re-send the copy of your card because the data cannot be viewed.

6 first digits.

Exchange of messages on Twitter from May 27 to June 8

of 2019 in which the claimant states that an order has been made that he

has not applied, that he is worried because the last digits of the card

match yours, that you wanted to access your account and couldn't, and

that the phone to recover the password is not yours. The claimed in

At first, he answers that the email provided does not correspond to

no account and they ask for an order number that you had made in the

past. The claimant provides them with the order number #GJPYLGSVC of

dated 01/06/2018 and the respondent replies that he is aware that the request is not

requested has been canceled without costs and that you will receive the amount charged

incorrectly. The complainant insists that he wishes to remove his data from the

application, for which you want to access it. To do this, the respondent

asks you to perform "a verification that we have sent to your email". The

claimant reproduces the mail in which they request a copy of the DNI and a copy of

the credit card associated with the account that shows your name and the 6

first digits and last 4 digits. The claimant indicates that he sent the photo,

but the claimed insists that the attached images cannot be

display the first six digits of the card and that they need that

information “in order to enable your profile”. The claimant refuses to provide

this data due to distrust in the security of the application, since

in February he had asked to delete the account and they had told him that

they would, but months later you get a message that an order was placed

from the account you had requested to delete. He states that he only wanted

access the application to remove your credit card number and that

you want to delete that account, along with all your personal data. Finally,

the respondent insists that he needs to verify his identity “to provide the

refund of the amount paid and then we can cancel the account”. The

Claimant answers that they had first told him that there was no account

with your email, after an order has been blocked with your account (the one that

had said it did not exist), they later told him that the money had been

returned and now they asked for more information to return the amount that was already

was returned, that it was clear that something was wrong or that the

claimed and that he was going to file a complaint with this Agency.

THIRD: in response to the requirements of this Agency, as well as during the

on-site inspection carried out and in his pleadings brief, the respondent has

stated that:

- The respondent acted with due diligence since the claimant received a

response to your email confirming receipt of your

application, which demonstrates that the claimant's application is carefully treated and

keep you informed about the status of your application.

- Regarding the measures adopted to avoid similar incidents: the claimed

lists the freezing and pseudonymization of the claimant's data, in accordance

with the aforementioned art. 17.3.e); the cancellation of the allegedly fraudulent order, despite

that this could be due to a possible hacking not attributable to the person claimed; and what do I know

proceeded to point out and block the user's entire profile, in order to prevent

possible fraud that could affect you. As improvement actions since 2018, the

claimed lists:

1. Change of the CRM software with which the relationship with customers is managed, for

from the application ***COMPANY.1 to ***COMPANY.2.

2. Maintenance and improvement of the platform that prevents fraud and blocking actions.

quea attempts that respond to a suspicious pattern.

3. Maintenance and improvement of the double authentication factor, eliminating the risk related

tive to inactive accounts whose mobile phone was not verified and the double factor was not

was activated.

4. Pseudonymization of data blocked on suspicion of fraud.

5. Application of verification measures for users with two accounts as a result of the

case ***CASE.1, which also reached the AEPD."

- At the end of 2018, a security measure was included in its application that

was that whenever a user authenticates from a new device,

sends a verification code to the mobile phone that you had entered during the

Discharge process. This process was already used during the registration process to verify

that the phone number entered was in the possession of the user.

- After the completion of each order, it is automatically verified if the operation

corresponds to some pattern of attempted fraud and, if so, appears

an alert for an employee of the respondent to block the account manually and

someone from the fraud department requests more information from the user via email

email in order to lift the blocking of the account. while the lockdown lasts

of the account, if the user tries to access his account, a message of

notice directing you to contact customer service; this message is seen in the

example of screenshot provided during the inspection.

- The user account with which the order was supposedly placed on May 27,

2019 has the date of creation in the information systems of the claimed person on 1
June 2018, and the erasure date is September 10, 2019. This is
shows the screenshots taken during the inspection in the database
data and in the administration platform of the person investigated on the request
KI17LG1HM and customer data ***ID.4, associated with that order.
- The events that occurred in relation to the claimant user's account coincide
fully with the usual behavior pattern of cybercriminals who use
data traded on the black market in Eastern European countries such as
Ukraine to impersonate the identity of its victims and make fraudulent purchases.
In this specific case, we will see that the cyberattack is carried out from Ukraine and that
takes advantage of the negligent action of the claimant, by repeatedly using the same
key in different services that were affected by a security breach that
exposed his credentials.
- The website haveibeenpwned.com offers a free service that allows anyone to
user to check if his email address appears on these lists, and therefore
So, if your keys have been compromised and you need to change them immediately. Yes
we introduce the address ***EMAIL.1 in this database, it is verified that the
The claimant's credentials have been exposed in five security breaches and
two attempts or indications of attack.
- The investigation also showed that the claimant had opened another account in
Glovo with the address ***EMAIL.2, delivery address and credit card (digits
matching initials and endings).
- The data of the claimant initially exposed in these lists was limited to the
email address and password, and, in the latest versions of
2019 the claimant's data had been enriched with much more data, which
include:

1. Geographic location

2. Employment data

3. Phone numbers

4. Profiles on social networks

5. Credit cards”

- The claimant is an exponent of scant diligence in the management and custody of his

credentials, as your history of keys exposed in security breaches is

starts in 2008 and runs through 2019, and the success of identity theft confirms

that during all this time the claimant has not changed the access codes

repeatedly engaged. In the Terms and Conditions that regulate the

service, available at https://glovoapp.com/es/legal/terms, Glovo warns users

users of their responsibility with respect to the choice of their passwords and when using

the Glovo app the user expressly accepts these obligations: “Clause 17. -

Users are fully responsible for the access and correct use of their profile and

other contents of the Platform subject to current legislation, whether national or

of the Country from which you use the Platform, as well as the

principles of good faith, morality, good customs and public order. Y

specifically, acquires the commitment to diligently observe these

General Conditions of Use.

Users are responsible for correctly consigning usernames and

individual, non-transferable and sufficiently complex passwords, as well as not

use the same username and password as on other platforms, all with

the purpose of protecting your account from fraudulent use by third parties unrelated to the

platform. (...)”

- The change of the CRM application destined to collect all the actions and

customer transactions prevents the claimant from having the logs with the details of

operations carried out in 2018.

- The claimed party deleted and blocked the claimant's data in an

correct and communicated the deletion to the claimant, for which it provides as

DOCUMENT 2 the screenshot extracted from the backup, in which

This confirmation appears.

In this Document 2, a table is attached in which you can see, among other things, the

Next information:

go

subject

submitter

comment

***ID.4

Elimination

account

***ID.4

Elimination

account

***ID.4

Elimination

account

C/ Jorge Juan, 6

28001 – Madrid

{'id':

116472211014,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

472211014.json',

'name': 'A.A.A.',

'e-mail':

***EMAIL.1',

'created_at':

'2018-01-

{'id':

116472211014,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

472211014.json',

'name': 'A.A.A.',

'e-mail':

***EMAIL.1',

'created_at':

'2018-01-

{'id':

116472211014,

'url':

'https://glovoservi

ce.*** COMPANY.

message

created at

2018-02-

01T19:39:3

4,000z

2018-02-

01T19:40:2

8,000z

Hello, I have been searching so much in the

application how on the website, and I have not

found nowhere way to

delete the account. I understand that this

It should be possible in a simple way

(although it is hidden), and if it cannot be

from the App that was from the page

Web. can you tell me how should i

proceed about it?

Hi A.A.A! goodbyes are always

tough, we don't want you to go! :(,

although we would like to know the reason why

which you have decided to leave, we care about you

opinion! If you have already thought it through and

want to delete your account, reply to this

email confirming the cancellation and we will manage

your request as soon as possible.

Remember that once processed, all your

data will be deleted and you will not be able to

access the details of

I confirm the deletion, thanks Greetings

On Feb 1, 2018, at 8:40 p.m., Glovo

<support@glovohelp.***COMPANY.1.com>

wrote:

2018-02-

01T19:44:1

8,000z

www.aepd.es

sedeagpd.gob.es

23/37

2018-02-

01T19:49:2

2,000z

solved in ***ID.4

I want to delete my Glovo account

2018-02-

01T19:45:3

0.000Z

Send

https://glovoapp.com/en/contact

since:

Hi A.A.A! goodbyes are always

tough, we don't want you to go! :(,

although we would like to know the reason why

which you have decided to leave, we care about you

opinion! If you have already thought it through and

want to delete your account, reply to this

email confirming the cancellation and we will manage

your request as soon as possible.

2018-02-

01T19:47:1

8,000z

On Feb 1, 2018, at 8:47 p.m., Glovo

<support@glovohelp.***COMPANY.1.com>

wrote:

Hi A.A.A! There is no going back :(

We confirm that we have deleted your

user account of our database

data. As we told you, not anymore

you will not be able to access your profile or the details of

your previous orders. The drop in shipping

from the newsletter to your email

will be effective in approximately 48

working hours

I want to delete my account, linked through

2018-02-

01T19:47:5

6,000z

2018-02-

01T19:48:4

3,000z

2018-02-

01T19:46:2

www.aepd.es

sedeagpd.gob.es

1.com/

api/v2/users/116

472211014.json',

'name': 'A.A.A.',

'e-mail':

***EMAIL.1',

'created_at':

{'id':

116472211014,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

472211014.json',

'name': 'A.A.A.',

'e-mail':

***EMAIL.1',

'created_at':

360237355414,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/360

237355414.json',

'name': 'A.A.A.',

'e-mail':

{'id':

360237355414,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/360

237355414.json',

'name': 'A.A.A.',

'e-mail':

'***EMAIL.3

360237355414,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/360

237355414.json',

'name': 'A.A.A.',

'e-mail':

{'id':

360237355414,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/360

237355414.json',

'name': 'A.A.A.',

'e-mail':

'***EMAIL.3

{'id':

116018503873,

***ID.4

Elimination

account

1511051 Disposal

account

1511051 Disposal

account

1511051 Disposal

account

1511051 Disposal

account

***ID.5

Elimination

account

C/ Jorge Juan, 6

28001 – Madrid

24/37

3,000z

2018-02-

01T19:48:1

0.000Z

2018-02-

01T19:48:4

8,000z

2018-02-

01T19:52:5

4,000z

***ID.5

Elimination

account

***ID.5

Elimination

account

***ID.5

Elimination

account

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

018503873.json',

'A.A.A.',

'yam':

'e-mail':

'***EMAIL.2

{'id':

116018503873,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

018503873.json',

'A.A.A.',

'yam':

'e-mail':

'***EMAIL.2

{'id':

116018503873,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

018503873.json',

'A.A.A.',

'yam':

'e-mail':

'***EMAIL.2

{'id':

116018503873,

'url':

'https://glovoservi

ce.*** COMPANY.

1.com/

api/v2/users/116

018503873.json',

'A.A.A.,

'yam':

'e-mail':

'***EMAIL.2

From Facebook,

Thank you

a greeting

---

since:

Send

https://glovoapp.com/en/contact

Hi A.A.A! goodbyes are always

tough, we don't want you to go! :(,

although we would like to know the reason why

which you have decided to leave, we care about you

opinion! If you have already thought it through and

want to delete your account, reply to this

email confirming the cancellation and we will manage

your request as soon as possible.

Remember that once processed, all your

data will be deleted and you will not be able to

access the details of

I confirm the deletion of the account, a

greeting

On Feb 1, 2018, at 8:48 p.m., Glovo

<support@glovohelp.***COMPANY.1.com>

wrote:

Hi A.A.A!

There is no turning back :(We confirm

that we have deleted your user account

from our database.

As we mentioned, you will no longer be able to

access your profile or the details of your

previous orders.

The cancellation of the sending of the newsletter to your

email will be effective in

approximately 48 business hours.

If you have any other questions at

respect, do not hesitate to contact us

replying to this same email.

- The change of the CRM application destined to collect all the actions and

customer transactions prevents the claimant from having the logs with the details of the

operations carried out in 2018, so his investigation has focused on verifying

or refute the four working hypotheses that it develops in its pleadings.

- A first hypothesis: that the cyber attacker used the credentials of the claimant,

unlocked and restored the old account. Indicates the claimed that to have made

the fraudulent request, the cybercriminal should have obtained permissions from

administrator and performed the following steps described and have circumvented all the

obstacles set up to prevent it:

It also points out that it would be absolutely disproportionate to mount such an attack

powerful to make a tiny order. For all these reasons, the respondent concludes that

This first hypothesis must be rejected.

- A second hypothesis: the claimant never verified his mobile phone number and the double factor authentication was left unactivated. Indicates the respondent that it is possible that an account that remains inactive for a few months (dormant account), move to a semi-lock mode and does not react to the delete command). The defendant alleges that “an account not verified and without the double factor activated coincides with a pattern of attempted fraud and therefore the account is blocked. This lock would be different from the post-deletion blocking, since in fraud attempts the blocked data remains in the main database because they must be consulted by the anti-fraud team to prevent further fraud attempts. However, this hypothesis does not fit with the fact that my client verified and confirmed in February 2018 that the account had been correctly suppressed.

- A third hypothesis: the cyber attacker created a new account using the address e-mail and credit card data of the claimant, obtained in the black market The respondent alleges that “The AEPD verified, during the course of the inspection at Glovo, and considers it a proven fact, that the fraudulent order

was made with an account that had been created on June 1, 2018. This is repeated several times in the agreement to initiate the sanctioning procedure and in the minutes of the inspection. This information is very important, because it shows that the account with which the fraudulent order was placed was not the same as the one created by the claimant. IS A DIFFERENT ACCOUNT.

The first account had the ID ***ID.1 and the second had the ID ***ID.3.

In addition, the first account used a MASTERCARD card and the second a card

VISA.

Let us remember that the proven facts begin in February 2018, when the

complainant requests the deletion of his account and the deletion of his data.

However, the checks carried out by the AEPD show that the account

used to place the fraudulent order was created FOUR MONTHS LATER

that the claimant requested the cancellation of his account and Glovo proceeded to

delete and block the data.

We understand that it was the cybercriminal who opened that account in June 2018 with

the data that it had obtained in the lists of e-mail addresses that were

they sell on the internet and on the black market.

This would certify that the deletion of the account and the blocking of the data was carried out

correctly, otherwise the cybercriminal would not have been able to use the

same email address.

The respondent indicates that, for this hypothesis to be feasible, there should have been

met the following requirements:

The respondent also alleges that it is notorious and widely known that, in the

deep internet black market, credit card data can be acquired

that have been exposed and that lists of accounts can be purchased with credit cards

credit not canceled after a security breach. And that the defendant defends that the

cyber attacker obtained the credit card data associated with the address of

claimant's mail on one of these lists.

To do this, it highlights two facts:

1. The claimant suffered a security breach in their Dropbox account, where

could keep your credit card details.

2. The claimant's details were on the enriched list that was discovered in

2019, but contained data from a higher age, which had been

enriched with contributions from other cybercriminals.

The defendant points out that Ukraine is also a country historically related to

phishing, so the ease of accessing credit card data is very

higher than that of other countries. And that, for all these reasons, he considers that the most probable option

It is possible that the cybercriminal used the claimant's credit card details

to place the fraudulent order, since the other options are much less

probable.

The respondent also points out that the charge related to the fraudulent order never reached

be made, since it was Glovo that detected a suspicious pattern and blocked the payment,

Therefore, no damage was caused to the claimant at any time.

Finally, the respondent indicates that, according to the evidence contained in the

procedure, obtained during the inspection at the Glovo offices, and provided

by the claimant and the respondent, the chronology of the events is as follows:

And it alleges that “This chronology fits perfectly with the proven facts and

demonstrates that my client acted diligently and without violating the regulations of

Data Protection.

The simple possibility that the events occurred in this way and not

As the Agency maintains, but does not prove, it allows my client to benefit from the

principle of presumption of administrative innocence and adopts as a hypothesis more

plausible that relating to the creation of a new account by the attacker, which in

at no time has it been contradicted by the Agency."

- A fourth hypothesis: the claimant opened a new account after the deletion

from the previous one. The defendant indicates that this hypothesis would not be unreasonable, since,

In addition to the Glovo account ***EMAIL.1, the claimant had the account

***EMAIL.2, of which he had forgotten its existence, or at least only exercised the

right of suppression in relation to one of them.

"For this reason, and despite the fact that the system logs do not keep the data from June

2018 to check the IP address from which the opening of this

new account, it is perfectly feasible that the claimant opened a new account

on June 1, 2018 and then forget that he had opened it.

This hypothesis would fully fit with the initial deletion of the data and the subsequent

identity theft by the cybercriminal, since the data of the

second account opened by the claimant would not have been deleted.

Remember that the IDs of the two accounts were different and the credit cards

also.

The chronology of events relating to this hypothesis would be as follows:

This timeline also fits the proven facts and shows that my

represented acted diligently and without infringing data protection regulations.

Also in this hypothesis, the simple possibility that the events occurred

in this way and not as the Agency maintains, but does not credit, allows my

represented to benefit from the principle of presumption of administrative innocence and adopts

The most plausible hypothesis is the one related to the creation of a new account by

of the claimant, which has never been contradicted by the Agency".

- In each of the working hypotheses considered by the respondent, they acted with

subject to the law and in no case kept the data of the claimant accessible to

persons other than those authorized to access the data blocked in the

datawarehouse.

Different firms of recognized prestige have issued, prior to the closing of

each of the funding rounds, status reports on compliance

company regulations (Due Diligence). The respondent has punctually complied with the

recommendations contained in said reports in order to ensure the protection

of the rights and freedoms of the interested parties.

In none of these reports has it been indicated that the respondent has

Insufficient security measures in relation to the authentication process of the

users.

- In relation to the continuous nature of the infringement, it has been proven that the cro-

nology of the facts maintained by the AEPD does not correspond to reality and that

no violation has occurred.

- In relation to the number of users, this is wrong, since the figure is very in-

lower and for the purposes of this procedure should be taken into account only the

active accounts. If it were true that it treats the data of more than 7 million customers

assets, it would be a great success to have had a single incident of these characteristics, since

that by simple statistical probability, human or computer errors throw ci-

far higher incident rates.

- He has acted at all times in good faith, using his best commitment, and without

never endanger the rights and freedoms of the interested parties. There does not exist, then,

a clear "intention" in failing to comply with current regulations since it carried out all

the necessary and due actions for compliance with the regulations and has adjusted

prudently his action to the law.

- The Glovo user account associated with the email address

***EMAIL.1, from which the fraudulent order was made, corresponds to ID ***ID.4.

- The query with ID ***ID.4 is a reference number created for the purpose

internal and organizational by the previous customer service provider

(*** COMPANY.1) that collaborated with Glovoapp23, S.L. at the moment the

user ***EMAIL.1 made the aforementioned query on February 1, 2018, as

it follows from DOCUMENT No. 2 provided in his letter dated 30

September 2020. Each reference number was intended to identify the

queries or incidents sent by the users of the claimed and that had to be

serviced by that provider.

- A change was made in the CRM software used to manage the relationship with its

customers in order to increase the security and reliability of the processes of

deletion and blocking of data. In this sense, said CRM change prevented him from having

the additional data about the query with ID ***ID.4 dated February 1,

2018. This is because the previous customer service provider

(*** COMPANY.1) had defined a retention period for the data of the

users that it dealt with in the name and on behalf of its clients (in this case,

Glovoapp23, S.L.) within a maximum period of 90 days from the end of the

of the contractual relationship, a term that has already passed.

- You have already provided this Agency with the information you had on the query with ID

***ID.4 made by the user ***EMAIL.1, as stated in his writing of

allegations dated September 30, 2020 and that he understands this information as

complete as it is composed, among other elements, of: reference ID number, route of

contact, query creation date, query type, subject, description and

content of the query, conversations held between the service agent

customer and user service, query chronology and user identification

***EMAIL.1 as the user who made the query".

FOURTH: the respondent is a large company in its business and development sector

of the business activity it performs requires continuous data processing

personal.

FOUNDATIONS OF LAW

Yo

The Director of the Spanish Agency is competent to resolve this procedure.

Data Protection, in accordance with the provisions of art. 58.2 of the GDPR and

in the art. 47 and 48.1 of LOPDGDD.

II

In the present case, the claimant claims that he had requested the deletion of his

Glovo account associated with your email ***EMAIL.1 in February 2018 and the

claimed had confirmed that said request was being processed. Nevertheless,

On May 19, 2019, you received a confirmation of a

order made that he had not requested, so he understood that the deletion of his

account requested by him had not been duly attended to and the account in question

had been active.

In this regard, article 17 of the RGPD "Right of suppression ("the right to be forgotten)"

establishes that:

"1. The interested party shall have the right to obtain, without undue delay, from the person responsible for the

treatment the deletion of personal data that concerns you, which will be

obliged to delete personal data without undue delay when any

of the following circumstances:

a) the personal data is no longer necessary in relation to the purposes for

those that were collected or otherwise treated;

b) the interested party withdraws the consent on which the treatment of

pursuant to Article 6(1)(a) or Article 9(2)

letter a), and this is not based on another legal basis;

c) the interested party opposes the treatment in accordance with article 21, paragraph 1,

and other legitimate reasons for the treatment do not prevail, or the interested party

object to processing pursuant to Article 21(2);

d) the personal data has been illicitly processed;

e) the personal data must be deleted for the fulfillment of a

legal obligation established in the Law of the Union or of the States

members that applies to the data controller;

f) the personal data has been obtained in relation to the offer of services

of the information society mentioned in article 8, section 1 (...)".

For its part, article 12 of the RGPD "Transparency of information, communication

and modalities of exercising the rights of the interested party" provides:

"(…) 2. The data controller will facilitate the interested party in the exercise of their

rights under articles 15 to 22. In the cases referred to in article 11,

section 2, the person in charge will not refuse to act at the request of the interested party in order to

to exercise your rights under articles 15 to 22, unless you can demonstrate

that it is not in a position to identify the interested party.

3. The data controller will provide the interested party with information regarding their

proceedings on the basis of a request under Articles 15 to 22, without

undue delay and, in any case, within one month of receipt

of the request. This period may be extended for another two months if necessary,

taking into account the complexity and the number of requests. The responsible

will inform the interested party of any of said extensions within a period of one month

from receipt of the request, indicating the reasons for the delay. When the

The interested party submits the request by electronic means, the information will be provided by

electronic means when possible, unless the interested party requests that it be

facilitate in another way.

4. If the person in charge of the treatment does not process the request of the interested party,

will inform without delay, and no later than one month after receiving the

request, the reasons for its non-action and the possibility of presenting a

claim before a control authority and exercise legal actions. (…)"

In the present case, if the request for deletion has not been duly processed

of the account would be treating the personal data of the claimant without having

law that legitimizes such treatment.

In this sense, article 5 of the RGPD "Principles related to treatment" establishes

that:

"1. The personal data will be:

a) processed in a lawful, loyal and transparent manner in relation to the interested party

("legality, loyalty and transparency");

b) collected for specific, explicit and legitimate purposes, and will not be processed

subsequently in a manner incompatible with those purposes; according to

article 89, paragraph 1, further processing of personal data for purposes

archive in the public interest, scientific and historical research purposes or

statistics shall not be considered incompatible with the initial purposes ("limitation

of the purpose»); (…)

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

in paragraph 1 and able to demonstrate it (“proactive responsibility”)”.

And article 6 of the RGPD "Legality of the treatment" provides:

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

conditions:

a) the interested party gave their consent for the processing of their data

personal for one or more specific purposes;

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

interested party is a party or for the application at the request of the latter of measures

pre-contractual;

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

applicable to the data controller;

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

of another natural person;

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

public interest or in the exercise of public powers vested in the controller

of the treatment;

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

pursued by the data controller or by a third party, provided that

over said interests do not prevail the interests or the rights and freedoms

fundamental data of the interested party that require the protection of personal data,

in particular when the interested party is a child.

The provisions of letter f) of the first paragraph shall not apply to the processing

carried out by public authorities in the exercise of their functions. (…)"

III

In the present case, the claimant had a Glovo user account associated with

your email ***EMAIL.1. According to DOCUMENT 2 that accompanies the letter

of allegations of the respondent, dated February 1, 2018, at 7:39 p.m. on

claimant requested the claimed to delete this account, by querying ID

***ID.4. The respondent, through his provider ***COMPANY.1 would have responded to

7:40 p.m. "Hello A.A.A.! Goodbyes are always hard, we don't want you

go! :(, although we would like to know the reason why you have decided to leave, we
your opinion matters! If you've already thought it through and want to delete your account, reply
to this email confirming the cancellation and we will process your request as soon as possible
possible. Remember that once processed, all your data will be deleted and you will not be able to
go back to access the details of the". At 7:44 p.m. the claimant would have answered
"I confirm the deletion, thanks Greetings." To this message, the claimant would not have
received subsequent response. However, the message "solved in ***ID.4" appears at
7:49 p.m. on the systems of ***COMPANY.1. It should be noted that it was not possible to obtain
the identification number of the user account associated with the query ID ***ID.4,
given that, as stated by the defendant in his allegations, the previous provider of
customer service of the complainant (*** COMPANY.1) had defined a
period of conservation of the data of the users that it treated in the name and by
account of its clients (in this case, the claimed one) for a maximum period of 90 days
counted from the end of the contractual relationship, a period that has already elapsed.
Nor has it been possible to determine the date of creation of this account.
On May 19, 2019, an order #GJPYLGSVC, with ID: ***ID.6, was placed from the
customer account ID ***ID.4, associated with email ***EMAIL.1. the claimant
communicated with the claimant, who canceled the order in question without generating expense
any for the claimant and proceeded to mark that account as fraudulent. According to
consists of the facts outlined, this account ID ***ID.4 was created on June 1,
2018 and deleted on September 10, 2019.
In addition to having an account associated with ***EMAIL.1, the claimant had a
account associated with your email ***EMAIL.2, with ID ***ID.1, linked to your
Facebook account. According to DOCUMENT 2 that accompanies the letter of
allegations of the claimed, on February 1, 2018 at 7:46 p.m. the claimant
requested the deletion of this account. The claimed, through its provider

***COMPANY.1, replied at 7:48 p.m. “Hello A.A.A.! goodbyes are always

tough, we don't want you to go! :(, although we would like to know the reason why

You have decided to leave, your opinion matters to us! If you have thought about it well and want

delete your account, reply to this email confirming the cancellation and we will manage your

request as soon as possible. Remember that once processed, all your

data will be deleted and you will not be able to access the details of the ". The claimant, to

at 7:48 p.m., he replied with the following message: “I confirm the deletion of the account,

a greeting". At 7:52 p.m., the respondent replied: “Hello A.A.A.! there is no turning back

back :(We confirm that we have removed your user account from our database

data. As we mentioned, you will no longer be able to access your profile or the details of your

previous orders. The cancellation of the sending of the newsletter to your email will be done

Effective in approximately 48 business hours. If you have any other query

in this regard, do not hesitate to contact us by replying to this same email.”

Although it is appreciated that in the query with ID ***ID.5, in which the deletion is requested

of the account ID ***ID.1 associated with the email ***EMAIL.2, once confirmed

the deletion by the claimant is answered confirming that it has occurred

that deletion of the claimed database, this is not the case in the query with

ID ***ID.4, in which the complainant requested the deletion of their user account

associated with the email ***EMAIL.1. In the latter, in DOCUMENT 2 that

is attached to the brief of allegations dated September 30, 2020, only

you can see a message that says “solved in ***ID.4”, without further details. therefore not

It has been proven in the file that such deletion would have been carried out

correctly or that it had not been done.

Analyzing the hypotheses raised by the defendant, it has not been proven either

that any of these hypotheses had actually occurred.

It is plausible that a cyber attacker would have obtained and used the credentials of the

claimant, since if the account had not been properly deleted, the system would

would have recognized and could have agreed and placed the order in question. Alleges the

claimed that "if the respondent's account had not been disabled, the attempted

access of the cybercriminal would have been neutralized by the double factor, since there was no

The cybercriminal received the SMS with the access code". And he adds that "the

investigation has found indications that the claimant may not have verified the number

mobile, so the double factor was not activated. This would be compatible with the scarce

diligence of the claimant in matters of computer security". In DOCUMENT 3

that accompanies your pleadings brief, the verification log is provided in which

it can be seen that the mobile device of the account used to

place the fraudulent order on May 27, 2019 at 11:14pm CEST. It is

i.e. the mobile device was verified after the creation of the account ID

***ID.4 and prior to placing the order not requested by the claimant. So,

it would not appear that the double factor had prevented access to the account.

It seems less plausible (although not impossible) that the claimant would never have

verified your mobile phone number and that the two-factor authentication had

remained without activating (second hypothesis) and that even so the account could have

used to place the fraudulent order. The pleadings explain that it is

It is possible that an account that remains inactive for a few months (dormant account),

go into a semi-lockdown mode and do not react to the delete command. Nevertheless,

in the allegations it is also explained that an unverified account and without the double

activated factor coincides with a pattern of attempted fraud and therefore the

bill. That is, if the claimant's account had not been properly deleted

and this had not activated the double authentication factor, the system would still

had been flagged as a pattern of attempted fraud and the account would have been blocked.

On the other hand, it is also plausible that a cyber attacker would have created a new

account using email address and credit card details

of the claimant obtained on the black market (third hypothesis). This is the hypothesis

defended by the defendant for the following reasons:

- The account from which the fraudulent order was made has a creation date of 1

June 2018.

- There is a first account with ID ***ID.1, with a MASTERCARD, and a

second account with ID ***ID.3, with a VISA card.

- There are no obstacles to creating a new account because the email address

The claimant's email had been suppressed and there was no

account duplication.

- The cyber criminal used his own mobile to install the application and the new

bill. Received the SMS on it and the account was verified. This check is

credited and occurred on May 27, 2019 at 11:14 pm CEST, according to

the system log. We attach as DOCUMENT THREE the verification log. By

that the claimant did not receive a verification SMS and that is why the claimant saw that the

mobile number on the account did not match yours.

- Being a new account, the cybercriminal put the address that he considered

timely for delivery

- The cybercriminal obtained the data of the card associated with the email address

claimant's email on the black market.

In this regard, it should be noted that the first account with ID ***ID.1 is associated with the

email address ***EMAIL.2. Therefore, it has nothing to do with the account.

subject of the fraudulent order, associated with the email address

***EMAIL.1. Even if the respondent had several accounts, they are accounts

independent.

The second account, with ID ***ID.3, has not been established as belonging to the

claimant nor what email address it was associated with. The

account that has been established as associated with the email address

***EMAIL.1 and from which the fraudulent order was made is the account ID

***ID.4. Nor could the ID of the account that initially had been established.

created the claimant with this email address.

Nor has it been proven that the cybercriminal who allegedly carried out the

fraudulent order would have used his own mobile and he would have verified the account in

question. Yes, it is stated in DOCUMENT 3 that accompanies the allegations of

date September 30, 2020, when this new account was created, the number was verified

of the mobile device associated with the account ID ***ID.4, on May 27, 2019 at

11:14pm CEST, prior to placing the fraudulent order.

Lastly, it has not been proven that a cybercriminal would have obtained

the details of the card associated with the claimant's email address in

the black market

However, if the claimant's account has not been deleted, the respondent alleges

that there would have been a duplication of accounts and a new one could not have been created

has the same address ***EMAIL.1. And yes, it has been established that the account

from which the fraudulent order was placed was created on June 1, 2018.

Finally, it is also plausible that the claimant opened a new account

after the suppression of the previous one (fourth hypothesis). The respondent alleges that “this

hypothesis would fit fully with the initial deletion of the data and the subsequent

identity theft by the cybercriminal, since the data of the

second account opened by the claimant would not have been eliminated.” In any

In this case, in order to have been able to create this new account, it should have been deleted

duly created previously or there would have been duplication of accounts and this does not

The defendant allows it, according to the allegations presented by him.

For all of the above, it has not been possible to duly prove in the file that the

deletion requested by the claimant had not been properly addressed and

had continued to process the claimant's personal data without a valid basis

law that legitimizes such treatment.

The foregoing must be connected with the validity of our Administrative Law

sanctioning the principle of presumption of innocence recognized in article 24.2 of

the Spanish Constitution, so that the exercise of the sanctioning power of the

State, in its various manifestations, is conditioned to the game of evidence and to

a contradictory procedure in which their own positions can be defended.

The principle of presumption of innocence prevents imputing an administrative offense

when proof of charge has not been obtained and verified that accredits the

facts that motivate the imputation or the intervention in the same of the presumed offender.

In the present case, there is no evidence that the deletion of your account, requested by the claimant, had not been attended to correctly and had continued to process the claimant's personal data without a legal basis that would legitimize such treatment, ignoring the applicable regulations.

The Constitutional Court (SSTC 131/2003 and 242/2005, for all) has ruled in that sense by indicating that one of the requirements inherent in the right to presumption of innocence is that the sanction is based on acts or evidence charge or incriminating the imputed conduct and that falls on the Public administration acting the evidentiary burden of the commission of the illicit administrative and the participation in it of the accused.

For its part, article 28.1 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector establishes as one of the principles of the sanctioning power the of "Responsibility" and determines in this regard that:

“Only those that constitute an administrative infraction may be sanctioned natural and legal persons, as well as, when a Law recognizes their capacity to to act, the affected groups, the unions and entities without legal personality and the independent or autonomous estates, which are responsible for them title of fraud or guilt”.

Likewise, the provisions of article 53.2 of Law 39/2015 must be taken into account, of October 1, of the Common Administrative Procedure of the Administrations Public, which establishes that:

In addition to the rights provided for in the previous section, in the case of administrative procedures of a punitive nature, the alleged responsible, will have the following rights: (...)

b) To the presumption of non-existence of administrative responsibility while

the contrary is not proven".

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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

Spanish Data Protection

RESOLVES:

FIRST: FILE procedure PS/00225/2020, initiated to the entity

GLOVOAPP23, SL, with CIF: B66362906.

SECOND: NOTIFY this resolution to the entity GLOVOAPP23, S.L.

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

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the

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

Interested parties may optionally file an appeal for reconsideration before the

Director of the Spanish Agency for Data Protection within a month from

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

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

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

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

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

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

aforementioned Law.

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-131120

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es