Registered

Booking.com B.V.

The board of directors

attn [CONFIDENTIAL]

PO Box 1639

1000 BP Amsterdam

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Subject

Decision to impose an administrative fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authoritypersonal data.nl

Dear [CONFIDENTIAL],

The Dutch Data Protection Authority (AP) has decided to ask Booking.com B.V. (Booking) an administrative

to impose a fine of € 475,000. The AP is of the opinion that Booking Article 33, first paragraph, of the

General Data Protection Regulation (GDPR) from January 16, 2019 to February 6, 2019

has violated, because Booking has failed to enter a personal data breach

to be reported to the AP 72 hours after becoming aware of this.

The decision is explained in more detail below. Chapter 1 contains an introduction and Chapter 2 describes it

legal framework. In Chapter 3, the AP assesses its authority, the processing responsibility and the violation. The (amount of the) administrative fine is elaborated in chapter 4 and chapter 5 contains the operative part and the remedy clause.

Attachment(s) 1

1

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

1 Introduction

1.1 Legal entities involved

Booking is a private company with its registered office at Herengracht 597 (1017 CE) in Amsterdam. Booking was founded on June 23, 1997 and is in the register of the Chamber of Commerce registered under number 31047344. Booking offers an online platform on which Trip Providers, such as accommodations, their products and services for reservation and users of the platform can then reserve it.

Booking is, through various Dutch and English legal entities, an indirect 100% subsidiary of aan de US NASDAQ Stock Market listed Booking Holdings Inc. The latter apparently had its 2019 public and consolidated financial statements reported sales of $15.1 billion (EUR 13,727,410,000) and a net result of USD 4.9 billion (EUR 4,454,590,000).

1.2 Reason for the investigation

On February 7, 2019, Booking reported a personal data breach to the AP (data breach) done. An unknown third party had gained access to a Booking system by posing as an employee of Booking at several accommodations. Here are the personal data of several parties involved, who make hotel reservations via the platform of Booking had done compromised. Because Booking has indicated that in the notification form

Booking had discovered the personal data breach on January 10, 2019, the AP is one

started an investigation into the compliance of Article 33, first paragraph, of the GDPR by Booking.

1.3 Process flow

In a letter dated 12 February 2019, the AP sent Booking a request for information. This request is

also sent by email on 26 February 2019.

On February 27, 2019, Booking has notified the above breach in connection with

personal data supplemented.

By letter dated 1 March 2019, Booking responded in writing to the request for information dated 12 February

2019.

By letter dated 6 March 2019, the AP sent Booking an additional information request.

By letter dated March 13, 2010, Booking responded in writing to the request dated March 6, 2019.

By email dated March 19, 2019, the DPA sent Booking an additional request for information.

By email dated March 19, 2019, Booking provided the requested information and an additional document to the

AP sent.

Due to the cross-border nature of the case, the AP has the other supervisory authority

authorities of the present case on March 19, 2019, which has also been established

that the AP acts as lead regulator now that Booking's head office is located in

The Netherlands.

In a letter dated 16 July 2019, the AP submitted an intention to enforce and the investigation report

Booking and Booking was given the opportunity to express its views.

By letter dated September 3, 2019, Booking has expressed its view in writing on this intention and

the underlying report.

On October 23, 2020, the AP submitted a draft decision to the data subject in accordance with Article 60 of the GDPR supervisory authorities. No objections have been lodged against this.

2. Legal framework

2.1 Scope GDPR

Pursuant to Article 2, paragraph 1, of the GDPR, this Regulation applies to the whole or in part automated processing, as well as to the processing of personal data contained in a file included or intended to be included therein.

Pursuant to Article 3, paragraph 1, of the GDPR, this regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, whether or not the processing takes place in the Union does not take place.

Pursuant to Article 4 of the GDPR, for the purposes of this Regulation:

1. “Personal Data”: any information relating to an identified or identifiable natural person (“the data subject”); […].

2. “Processing”: an operation or set of operations relating to personal data or a set of personal data, whether or not carried out by automated processes […].

7. “Controller”: a […] legal entity […] that, alone or jointly with others, carries out the purpose of and determines the means for the processing of personal data; […].

12. “Personal Data Breach” means a security breach that occurs accidentally or on unlawfully leads to the destruction, loss, alteration or unauthorized disclosure of or unauthorized access to data transmitted, stored or otherwise processed;

[CONFIDENTIAL]

23. “Cross-border processing”: […] b) processing of personal data in the context of the

activities of one establishment of a controller […], resulting in more than one

Member State data subjects are or are likely to be materially affected.

2.2 Notification of personal data breach

Pursuant to Article 4(12) of the GDPR, a “personal data breach” means

means a breach of security leading to the accidental or unlawful destruction,

the loss, alteration or unauthorized disclosure of or unauthorized access to

transmitted, stored or otherwise processed data.

Pursuant to Article 33(1) of the GDPR, a controller submits a breach

relating to personal data without undue delay and, if possible, no later than 72

hours after he has become aware of it, to the supervisory authority competent in accordance with Article 55

authority, unless the infringement is unlikely to result in a risk to the rights and freedoms

of natural persons (…). In case the notification to the supervisor is not made within 72 hours

takes place, it shall be accompanied by a justification for the delay.

2.3 Competence leading supervisory authority

Pursuant to Article 55, paragraph 1, of the GDPR, each supervisory authority has the competence to

territory of its Member State to carry out the tasks assigned to it in accordance with this Regulation

and to exercise the powers conferred on it in accordance with this Regulation.

Pursuant to Article 56, paragraph 1, of the GDPR, the supervisory authority of the principal place of business or the

any establishment of the controller (…) without prejudice to Article 55, to act competently

as the lead supervisory authority for cross-border processing by those

controller (…) in accordance with the procedure set out in Article 60.

3. Review

3.1 Competence AP

In the present case, it concerns a processing of personal data by Booking

data subjects have been substantially affected in more than one Member State.1 As a result, there is cross-border processing within the meaning of Article 4, part 23 sub b, of the GDPR. The AP states established that it is competent to act as a lead supervisory authority pursuant to Article 56 of the GDPR authority now that Booking's headquarters is located in Amsterdam.

1 See section 3.4.2 for this.

3.2 Processing of personal data

According to Article 4(1) of the GDPR, personal data is any information about a identified or identifiable natural person (“the data subject”). If becomes identifiable considered a natural person who can be identified directly or indirectly, for example by one or more elements characteristic of the physical or physiological identity of that natural person.

Article 4(2) of the GDPR defines the concept of processing as an operation of personal data, such as collecting, recording, storing, retrieving, consulting or using it.

Booking offers an online reservation platform where so-called "Trip Providers", such as accommodation providers and other providers, available accommodations, flights, rental cars and offer day trips. Via the platform, visitors can, among other things, go to overnight addresses and search for day trips, after which they can be reserved via the platform.

When making a reservation via the Booking platform, the person concerned collects personal data such as contact, reservation and payment details entered. Booking then provides the details of the reservation to the Trip Provider via the Extranet of Booking. 2 The Booking Extranet is an online administrative dashboard with secure access. In addition to access to reservation data in the Extranet,

the Trip Providers have access to all information provided on the Trip Provider page at Booking.com displayed, including the payment options and policies.

To gain access to the Extranet, the Trip Provider must provide a username, password and 'two factor authentication pin code'. After the Trip Provider has logged in to the Extranet, they can access the consult necessary reservation data of the guests.

Booking's Security Team, which was called in as a result of the breach, has determined that a unknown third party has gained access to the Booking Extranet. The findings of the Security Team are recorded in a so-called Security Incident Summary report. From it in the file recorded Security Incident Summary report dated February 28, 2019 shows that, among other things, the following guest data stored in the Extranet has been compromised: first name, last name, address, telephone number, check-in and check-out date, total price, reservation number, price per night, any correspondence between accommodation and guest and with regard to those involved the credit card details of which 97 with the 'card verification code'.3

The reported personal data breach of Booking therefore concerns, among other things, names, address details, telephone numbers and credit card details of hotel guests. Now this information concerns about identified or identifiable natural persons, the aforementioned data can be regarded as personal data as stipulated in Article 4, first part, of the GDPR.

2 File document 1: notification of personal data breach 7-2-2019, p3.

3 File document 9, Responses from Booking to request for information, Annex 5.

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

The AP has established that processing of personal data takes place via the Extranet: the data are recorded in the Extranet, stored and further made accessible. The set of operations in the

Extranet is a processing of personal data as referred to in Article 4, part two, of the GDPR.

3.3 Controller

In the context of the question of who can be held responsible for committing an offence of the GDPR, it should be determined who can be regarded as the controller as referred to in Article 4(7) of the GDPR. It is important to determine who is the target of and the means of processing personal data – in this case the processing of personal data of data subjects who use the Booking platform.

The AP is of the opinion that Booking determines the purpose and means for the processing of the personal data relating to reservations made via Booking.com and subsequently processed via the Booking Extranet. The AP explains this as follows.

Booking's Privacy Statement, as posted on its website, states which personal data are processed by Booking as well as the reasons why and the way in which this is done are processed. The Privacy Statement states, among other things, that Booking shares data with third parties, including the “Trip Provider”, or the Trip Provider. That the data will be shared with the travel provider shared via the Extranet is apparent from, among other things, the notification of the breach on 7 February 2019 and the view of Booking.4 The Privacy Statement also explicitly states that the processing of the above said personal data is done by Booking (Herengracht 597, 1017 CE Amsterdam, Netherlands).5

In addition, Booking determines the details of the security of the Extranet by making arrangements security measures for access control such as the “two factor authentication” (of which the code is also generated by Booking).6 In addition, Booking has, among other security measures, set up a data breach reporting procedure that pertains to incidents concerning the Extranet.7

Based on the aforementioned, the AP therefore concludes that Booking determines the purpose and means for the processing of personal data relating to reservations made via the platform of Booking are made through the Extranet (a system used by Booking and managed) are processed.

Booking has argued in its opinion on the one hand that Booking is the controller

for the customer data processed in relation to its platform.8 On the other hand, Booking

4 File document 20: research report, marginals 17 et seq., opinion marginals 2.3 et seq.

5 Under the heading “Who is responsible for the processing of personal data via Booking.com and how to reach us?”.

6 Opinion, marginal 2.5.

7 Opinion, marginals 2.6, 3.2 and 3.3.

8 Opinion, marginal number 2.2.

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

that the Trip Provider acts as the controller for the customer data sent via the Extranet

are made available and that Booking does not consider itself responsible for

data processing activities of the Trip Providers.9

That Trip Providers can also access the Extranet (physically) and process personal data therein,

does not alter the fact that Booking is the controller for the Extranet. And thus also

responsible for what happens to the personal data in the Extranet. The argument from

Booking therefore fails.

That Booking also sees itself as the controller for the personal data that is processed via the

Extranet, is also apparent from the fact that Booking committed the infringement in connection with

reported personal data to the AP on February 7, 2019 and also states in its opinion Booking

be the controller for the customer data processed through its platform.10

Based on the foregoing, the AP determines that Booking is the controller in the sense

of Article 4, part seven, of the GDPR.

3.4 Reporting Infringement Violation

3.4.1 Introduction

Article 33(1) of the GDPR stipulates that if a personal data breach has occurred

occurred, the controller will do so without undue delay and, if possible,

to the (…) competent supervisory authority no later than 72 hours after becoming aware of it

unless the personal data breach is unlikely to pose a risk

for the rights and freedoms of natural persons. In case the notification to the supervisor is not

takes place within 72 hours, it shall be accompanied by a justification for the delay.

In this section, the DPA will first outline the facts and then assess whether Booking has committed the infringement

should have reported (in a timely manner) to the supervisory authority.

3.4.2 Facts

January 9, 2019

On January 9, 2019, a property 11(I) in the United Arab Emirates reports to a

[CONFIDENTIAL] of Booking by email that a guest complained about being emailed

was approached by an unknown party posing as an employee of the property with the

notification that their credit card did not work and whether the guest provided his date of birth or other bank card details

wanted to give up so that a reserved overnight stay could be paid in advance. The accommodation manager

asks in his email message to Booking to investigate the incident now the property from the

Extranet does not have customer email addresses and he thinks that is probably the case

9 Opinion, marginal number 2.3.

10 Opinion, marginal number 2.2.

11 In other words: a Trip Provider.

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

a (data) leak at Booking since the unknown party was aware of the, via the platform of

Booking made, reservation at the property.

Email dated January 9, 2019 6:00 PM

“Good Afternoon […],

We received a complaint from a guest stating that he had provided his personal information and credit card information to a 'stranger' posing as a Reservations employee of our property […]. In the 1st attachment a person by the name of [CONFIDENTIAL] had directly email the guest (from a Hotmail account) requesting his credit card and personal info to pay for his booking. We are not sure if the guest had sent the details about it. We got to know when someone from B.com called

the property to check if anyone had sent the email. We contacted the guest via the phone number listed in the reservation form – he forwarded the [CONFIDENTIAL] email to us. As we do not get guest email address from the extranet, the issue here is likely to be from B.com. We don't know how this [CONFIDENTIAL] managed to get hold of the guest email and that he had made a booking at our property from B.com. Can you review and share the outcome with us. Guest has the perception and understanding that we had leaked the information which is not true. Our brand confidence is at stake here, so is B.com.

Kind regards […]"

The e-mail that the person concerned had received from the unknown third party was attached to the aforementioned e-mail received. This email shows that the unknown third party is using the reservation details

attempts to obtain personal and/or payment data from the data subject.

Email dated January 8, 2019 10:32 PM

“Dear Sir

My name is […] and this email is regarding your booking in out hotel. We got your email address from your office actually sir your bank card is not working. Ever time we attempted the payment it on terminal it is asking for card holder date of birth. Kindly provide us with your date of birth or a different card no so we can take the initial deposit of 1 night in order to guarantee the booking rate for 1st night is 450 emarati dirhams.

Many thanks

[…]

reservation department”

January 13, 2019

On January 13, 2019, the same accommodation (I) reports to the aforementioned [CONFIDENTIAL] of Booking that a similar complaint has been received from another guest. An unknown party had intervened – this time by telephone – made known to the guest on behalf of Booking where an attempt was made to charge their credit cards obtain personal data.

Email dated January 13, 2019 10:18 am

“Subject: RE: [External Fraud] / Leaked Guest Information / URGENT

Hi […]

8/27

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

We receive a complaint from another guest…this time someone claiming to be from B.com (UK number) called the guest and was trying to get his cc and personal details for 1 night charge.

I am not sure if the guest provided his details, but he contacted us which we clarified the same (similar clarification as our 1st case). We had requested the guest to call B.com instead.

We had taken precautions by changing all our logins (for those who has access) last week Thursday.

Booking No. […]

Regards

[…] [CONFIDENTIAL]”

January 20, 2019

On January 20, 2019, Property I reports that a third guest has complained about being on the phone approached with a request to provide his credit card information. The accommodation manager indicates

the [CONFIDENTIAL] of Booking that given the seriousness of the situation will become the issue

scaled up to headquarters.

Email dated January 20, 2019 5:14 PM

“Subject: RE: [External] Fraud / Leaked Guest Information /URGENT

[…]

Hi […]

We receive another complaint from a guest about someone calling them to get cc details. Below is his booking – we have advised him to contact B.com.

As it looks serious now, we are escalating the issue to our head office in Singapore.

Kind regards,

[…] [CONFIDENTIAL]”

Also on January 20, 2019, a second accommodation reports to Booking that there is “an

alarming situation with Booking.com reservations”. Various guests who had reserved via Booking,

have been contacted by telephone with the request to provide their credit card details. Also this accommodation

asks Booking's [CONFIDENTIAL] to investigate.

Email dated January 20, 2019 11:35 am

“Good morning […]

We have an alarming situation with Booking.com reservations. The last couple of days, we have guests reserved through booking.com, contacting us to inform us that someone from our in-house reservations department called them to get their credit card details for their reservations. The person who calls the guests knows their reservation details (arrival/departure etc.). Attached and below you can find more details about this matter.

We have already changed the [CONFIDENTIAL] password as well as my own password.

Can you please look into this?

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

Thank you,

[…]

[CONFIDENTIAL]"

Booking has a policy that suspicions and reports of incidents must be reported immediately

forwarded to the Security Team of Booking.12

The [CONFIDENTIAL] of Booking that were notified by the accommodations of the

fraudulent acts by an unknown third party have the Security Team of Booking on

January 31, 2019 informed.

On February 4, 2019, Booking's Security Team completed and concluded its first investigation

that Booking's Privacy Team should be informed. The research findings of the

Security Team are documented in the aforementioned February 28 Security Incident Summary Report

2019.13

This investigation by the Security Team revealed that 40 accommodations in the United Arab

Emirates have become victims of social engineering fraud involving the personal data of

possibly 4109 data subjects have been compromised. An unknown third party has turned up

pretended to be a Booking employee over the phone to obtain the username, password and two-

factor authentication code (“2FA”) from the accommodations. With this information, the third party

party to log in to the Extranet of Booking, which contains reservation data of guests.

The Security Team has determined that December 19, 2018 is the start date of the security incident

been. The persons involved came from Europe (including Great Britain,

France, Ireland, Switzerland, Belgium, the Netherlands) as well as from other parts of the world (including South

Africa, America, Canada and Bahrain).

The personal data concerned included first name, last name, address, telephone number,

check-in and check-out date, total price, reservation number, price per night, any correspondence

between accommodation and guest and credit card details with regard to 283 data subjects, of which 97 with the 'card verification code'.

On February 4, 2019, the Security Team informed Booking's Privacy Team about the outcomes of the investigation. All parties involved were also informed by Booking on 4 February 2019 brought.14

Booking's Privacy Team determined on February 6, 2019 that there had been a data breach that had to be reported to the AP.

12 See file document 15, Response to request for information regarding internal policy documents on data breaches.

13 File document 9, Responses from Booking to request for information, Annex 5.

14 Notification form and opinion, marginal number 4.4 under d.

On February 7, 2019, Booking submitted a notification to the AP as referred to in Article 33, paragraph 1, of the GDPR.15

3.4.3 Assessment

Article 33(1) of the GDPR stipulates that if a personal data breach has occurred occurred, the controller will do so without undue delay and, if possible, to the (…) competent supervisory authority no later than 72 hours after becoming aware of it unless the personal data breach is unlikely to pose a risk for the rights and freedoms of natural persons.

Before the notification is made, the controller must therefore first be informed assesses whether there has been a personal data breach. Then it should be assessed whether the breach poses a risk to the rights and freedoms of natural persons.

A personal data breach

As the DPA has established in paragraph 3.4.2, an unknown third party has had access to it
Extranet of Booking and thus gained unauthorized access to the data processed by Booking
data related to guest reservations at accommodations. Booking does not dispute that either
there was a personal data breach. The AP thus establishes that there is
of a personal data breach within the meaning of Article 4(12) of the GDPR.

Risk to the rights and freedoms of natural persons

After the unauthorized acquisition of the aforementioned personal data, the unknown third party
then attempted to obtain credit card information from using this personal data
guests who had booked through Booking's online platform. With this, the AP not only establishes that
it is likely that the personal data breach poses a risk to rights
and freedoms of natural persons but also that this risk has materialized now the unknown
third party has contacted many, if not hundreds, of data subjects to try them on
to steal credit card information on the basis of improper grounds. Due to the violation of the
confidentiality of the data was not only a risk of financial damage but also of
identity fraud or any other disadvantage. The AP therefore establishes that the infringement is related to
personal data posed a risk to the rights and freedoms of natural persons.

Reporting to the supervisory authority competent in accordance with Article 55

It has been established in paragraph 3.3 that Booking is the controller. In section 3.1, the AP
established that it is competent to act as a leader pursuant to Article 56 of the GDPR
supervisory authority now that Booking's headquarters is located in Amsterdam. Booking has
reported the breach to the AP on January 7, 2019. Booking has therefore reported this to the in
competent authority in accordance with Article 55 of the GDPR in this case.

15 File document 1, Notification of personal data breach 7-2-2019. P5.

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

Notification no later than 72 hours after the controller becomes aware of a breach related to

personal data

The Guidance on Personal Data Breach Notifications under Regulation

2016/67916 (hereinafter: Guidelines), prepared by the Article 29 Data Protection Working Party (hereinafter:

WP29), contain an explanation of the notification obligation(s) in the GDPR and provide guidance on how to do this in various

types of infringements must be acted upon.

When exactly can a controller be considered to have become aware of

a particular breach depends on the circumstances of the specific breach. According to the WP29

a controller shall be deemed to have become aware of a related breach

with personal data when he has a reasonable degree of certainty that a security incident has occurred

occurred that led to the compromise of personal data.

The DPA is of the opinion that Booking was aware of the infringement in connection with

personal data and considers the following to this end.

On January 9, 2019, the [CONFIDENTIAL] from Booking received a first signal, via an email

from a Trip Provider in the United Arab Emirates (accommodation I) that is included with the

the person involved and the Trip Provider had a serious suspicion that there was a data breach. The

The person concerned was approached via e-mail on 8 January 2019 by a third party (who remained unknown).

was with the reservation made via the Booking platform and on the basis of that

reservation details tried to obtain more personal data with which supposedly a payment of

an overnight stay could be arranged. From the conscious email dated January 8, 2019, which is

included in the file, it appears that it also contained a PDF file with the reservation details. This

pdf file was not submitted by Booking and therefore not included in the file.

In the opinion of the AP, the aforementioned incident should have been handled by (the [CONFIDENTIAL] of) Booking

will now be forwarded to the Security Team of Booking for further investigation into the email

matter contained the exact reservation details of the person concerned and it was also established that the booking was made through the

platform of Booking was created. All the more so now that the Trip Provider had already come to the conclusion that there had to be a security incident and on the basis of the data available to him

had already made an initial assessment. This is also apparent from the information given by the accommodation manager subject of the email: “[External] Fraud / Leaked Guest Information/ URGENT”. The Security Team had

an exploratory investigation could already be started at that time.

On January 13, 2019, (the same [CONFIDENTIAL] of) Booking received a second signal from

said Trip Provider. The data subject in question was asked for his personal data by telephone

by someone posing as an employee of Booking who was aware of the

the reservation made via the Booking platform. The accommodation manager has in his e-mail

e-mail to the [CONFIDENTIAL] of Booking expressly stated that it considers the incident equivalent

16 Guidance on personal data breach notification under Regulation 2016/679, Working Party

Data Protection Article 29, last revised and adopted on February 6, 2018, 18/EN WP250rev.01.

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

to the earlier incident and again believed that there must have been a data breach on the part of

booking.

The AP is of the opinion that Booking is deemed to have knowledge of the

breach in connection with personal data, because Booking has a reasonable

degree of certainty that a security incident has occurred that led to the compromise of

personal data processed by Booking. The Trip Provider's accommodation manager

after all, had already concluded that there must have been a security incident with regard to

the Extranet, where guest personal data had been compromised.

Given the alarming situation, Booking should have immediately reported the incident to the Security Team

of Booking so that an investigation into the scope of the infringement could be carried out, which, however, was done by

Booking until January 31, 2019 failed.

Based on the foregoing, the term of 72

hours for reporting a breach to the AP started on January 13, 2019. As a result

Booking should have reported the personal data breach to the DPA by 16 January 2019 at the latest

report. It has been established that Booking did not make this notification until February 7, 2019, therefore 22 days too late.

This also applies if the date 20 January 2019, the date on which next

accommodation I also located another Trip Provider (accommodation II) in the United Arab Emirates

Emirates has reported to Booking's [CONFIDENTIAL] with similar incidents. Also in this one

e-mail notifications, the subject is garishly capitalized: **SECURITY

BREACH**. In that case, the personal data breach would be delayed by 15 days

supervisory authority have been reported.

3.4.4 View of Booking and response by AP

Infringement notification

In its view, Booking has primarily taken the position that there is no question of a

violation since it only took note on 4 February 2019, after completion of the internal investigation

of the breach after which it is timely and without unreasonable delay within 72 hours of becoming aware of it

reported, which according to Booking is in line with Article 33, first paragraph, of the GDPR.

The AP does not follow this point of view. As can be seen from the foregoing, the AP has determined that Booking on 13

became aware of the infringement in January 2019. It follows that Booking committed the infringement in connection with

has not reported personal data in accordance with the provisions of Article 33, first paragraph, of the AVG.

Accommodation notifications

With regard to the signal from accommodation I on January 9, 2019, Booking has its view

argued that the [CONFIDENTIAL] of Booking had considered at the time that no

there was reason to scale up the report to Booking's Security Team, because the

the person concerned had been approached by e-mail. Booking states that email addresses in the Extranet are

hashed and cannot be extracted from it. Furthermore, Booking argues that the affected

accommodation and the [CONFIDENTIAL] of Booking would have come to a joint conclusion

that “it was probably not an incident at Booking”.

With regard to the latter, the AP notes that in addition to the fact that no substantiation has been provided for this

in the opinion, it is established that the [CONFIDENTIAL] of Booking has not acted according to its own

protocol of Booking, whereby any suspicion of an incident must be immediately passed on to the

Booking security team. The AP believes that despite the fact that e-mail addresses are

hashed in the Extranet, the aforementioned incident should have been forwarded to Security by Booking

Team. After all, the fact that the e-mail in question contained the exact reservation details of the person concerned and

the fact that the booking was made through Booking's platform had the [CONFIDENTIAL] of

Booking must alert and induce further action.

With regard to the incident of January 13, 2019, Booking argued that the [CONFIDENTIAL] in

issue did not see any direct similarities with the previous incident, so not to a reasonable degree

it could be stated with certainty that a security incident had occurred at Booking.

However, the AP is of the opinion that the fact that the (accommodation manager of the) Trip Provider already had

considered that there was an equivalent incident and that the security incident had to be made

have with the Extranet, for which Booking is the controller, that makes Booking on that

knew with a reasonable degree of certainty – and therefore had knowledge – that an infringement was taking place

occurred in connection with personal data. Also in this case were the exact reservation details
known to an unknown third party who falsely pretended to be an employee
from Booking.com. At this point, Booking had reasonable assurance of the security incident
where personal data had been compromised. It was highly certain that these data matter
a platform used by Booking for the benefit of its business activities had been obtained, it now appears
the e-mail correspondence according to the Trip Provider and the data subjects in question could be excluded
that a security incident had occurred on their side.

Violation of internal duty to report

Booking has further argued that it cannot be held against Booking that the procedure for
reporting security incidents, which means that security incidents are reported by the Trip Providers through the
so-called “Partner Portal” must be reported to the Security Team of Booking, by the
accommodations in question17 has been violated. According to Booking, violating that reporting obligation and the
fact that the [CONFIDENTIAL] of Booking did not immediately escalate to Booking as
company are challenged. Booking pointed to a decision by the Hungarian
privacy regulator, who would have ruled that negligence from only one part of the
organization cannot be enforced against the entire organization if appropriate measures were taken
affected.18

17 In this case, the accommodations in the United Arab Emirates.

18 Penalty decision Hungarian National Authority for Data Protection and Freedom of Information of 21 May 2019,
NAIH/2019/3854.

The AP states first and foremost that Booking, as the controller, has the obligation to inform each

alarming signal to investigate a possible security breach

personal data, so that action can be taken in a timely manner and in line with the provisions of the GDPR if there are any

a personal data breach has occurred. According to the AP, this is separate from any

private law agreements that Booking may have made with a third party on that point, such as in

in the present case the relevant Trip Providers. From paragraph 5.1 of the

“Data Incident Response Policy” also shows that all suspicions of incidents, even if they pass

“third party service providers” as the Trip Providers mentioned have been reported to Booking, must immediately

are forwarded to the Security Team of Booking:

“Prompt Reporting

All (suspected) Data Incidents must immediately be reported to the Booking.com security team (“Security”). This

includes Data Incidents notified to Booking.com from any third party service providers or business partners or

other individuals. (…)”.

On 9, 13 and 20 January 2019, various data incidents were reported by the accommodations to

(the [CONFIDENTIAL] of) Booking, which, however, has not led to the – in its own proceedings

recorded - required notification thereof to the Security Team. Already on January 13, 2019, the

[CONFIDENTIAL] of Booking aware of the breach, despite the fact that the Security Team was only on 31

notified in January 2019.

Insofar as Booking has an appeal with reference to the decision of the Hungarian regulator

want to do on the principle of equality, the AP notes that this case is not only about an infringement

of a completely different order, namely a breach of the confidentiality of personal data

the same organizational unit (of a government body) and not a case of “social engineering”

where there is a form of fraud, but also that the AP in that decision has a different opinion of the

supervisor then reads has been outlined by Booking. The fact that in that case the notification was made too late

an infringement as referred to in Article 33, first paragraph, of the AVG because an employee was late

is continued, contrary to what Booking suggests, the organization in question is indeed through the

Hungarian regulator.

Personal privacy risk

Booking has furthermore argued that the investigation report wrongly includes a risk to the personal privacy has been adopted without making an analysis of the terms and conditions implemented by Booking security measures aimed at protecting privacy and removing adverse consequences and has given a number of examples.19

19 Examples mentioned: if a data breach occurs, this is generally limited to contact details, without e-mail email addresses, and reservation dates; credit card information is stored according to PCI DSS standards; customers are informed about social engineering and other forms of fraud; data subjects were informed immediately after the data breach was discovered and advised and Booking has indicated that it will compensate all damage suffered.

The AP does not follow the latter position of Booking. As soon as personal data, as in this case, is added to end up with an unauthorized person and have been viewed, there is already a risk to rights and freedoms of natural persons. This risk has also manifested itself in the present case now that the data subjects had been approached by an unknown third party who unlawfully disposed of the personal data of those involved. That Booking subsequently promised to cover any financial damage compensation does not detract from the fact that the personal data has ended up in the wrong hands. It the risk of any consequences of the infringement has not thereby been removed.

Notification within 72 hours

Booking has further argued that making a notification within 72 hours as referred to in Article 33, first paragraph of the GDPR is not always possible. It can take specialized security teams for weeks or more

months to connect “data points” and conclude that a pattern of facts is indeed a
data breach that must be reported. Furthermore, it would be incorrect and inconsistent with the
AVG if the AP would expect Booking to generally take only three days to get a
conduct investigations and become aware of a personal data breach. In addition
according to Booking, the WP29 explicitly states in its Guidelines that it may take a while before
a controller can determine the extent of the breaches and the
controller can better prepare a meaningful report in which several, strongly related
similar violations are combined rather than reporting each violation separately. Finally has
Booking argued that the investigation report erroneously considers that Booking has no
has given valid reasons for the (alleged) violation of the 72-hour period. In the notification of
February 7, 2019, clear reasons are given, based on the thorough investigation by Booking,
whereby Booking reiterates that it primarily takes the position that notification has been made within 72 hours
after becoming aware of the personal data breach.
The AP is considering the following in this regard.
The AP endorses the position that an investigation into the scope and precise merits of an infringement
may take longer than 72 hours. Because it is not always possible to have all of them
necessary information about a breach enabling a notification to be made that complies with all
requirements laid down in Article 33, third paragraph, of the GDPR, the possibility to do a
notification in steps included in the GDPR. This possibility is in Article 33, fourth paragraph, of the GDPR
captured. This does not alter the fact that the notification of the infringement pursuant to Article 33(1) of the
AVG must take place within the legally prescribed period of 72 hours. As in section 3.3.3
already noted, Booking should be deemed to have become aware of the
personal data breach. That the infringement pursuant to Article 33, first paragraph, of the GDPR
should have been reported, it was then also clear. Booking has taken too long in this case
waited before making the notification prescribed in Article 33, first paragraph, of the AVG. The thorough
research to which Booking refers in no way justifies the delay in the aforementioned (initial)

notification, which therefore constitutes an unreasonable delay as referred to in Article 33, first paragraph, of the AVG.

16/27

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

Meaningful notification

With regard to what has been argued by Booking with regard to the preparation of a meaningful notification in which several similar infringements are reported together, the AP is considering that the point in the present case is that Booking was already aware of the infringement on 13 January 2019 and should have made the – initial or otherwise – notification in a timely manner. That there would be several on top of each other here seeming infringements that, according to Booking, could be packaged in one meaningful report, the AP considers to what has been considered above, in section 3.4.3 – not relevant.

Justification delayed notification

Booking has argued that outside the Guidelines there are no instructions that indicate with what arguments a delayed notification can be justified and that the AP is a new standard cannot be applied retroactively. Moreover, the AP could have asked for the delay to explain in more detail.

The AP considers that there is no retroactive application of a new one norm. The regulation included in the GDPR on this point is clear: when there is a breach of in connection with personal data, it must be processed without unreasonable delay, and if possible, no later than 72 be reported to the supervisory authority hours after becoming aware of it. The Guidelines give to it interpretation of the AP judgment for compliance with the reporting obligation(s) included in the GDPR of infringements; they can therefore by no means be assessed as a new standard. By the way, it is all

time on the path of the controller to a report that cannot be made in time,

provide adequate justification.

Practical implications AP judgment

In its opinion, Booking has also expressed its concerns about what it considers to be the practical implications of the opinion of the AP in the investigation report.20 The strict explanation mentioned therein brings according Booking entails that all potential security incidents, where there is a chance that

personal data is compromised, must be reported within 72 hours and that the Security

Team every complaint that comes to Booking - regardless of the way and content - must be

to research. In addition to an unreasonable and unrealistic administrative burden, this would also

unreasonable and unrealistic financial burden.21 [CONFIDENTIAL]. If all individual

complaints should be investigated immediately, as the AP advocates, would be considerably more

manpower than now. Such unreasonable organizational measures, with accompanying

disproportionate implementation costs go against the idea behind the security obligation of

Article 32 of the GDPR, according to Booking.

20 In paragraph 5 of the opinion.

21 [CONFIDENTIAL]

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

The AP assumes that the GDPR prescribes which obligations Booking has to fulfill in its capacity as

controller must comply. Pursuant to Article 32 of the GDPR, a processing

the responsible party is obliged to take all appropriate and organizational measures to mitigate the risk

to ensure an appropriate level of security: the ability to detect a breach in a timely manner, to

catch and report should be considered an essential part of these measures.22

According to the AP, it does not follow from the investigation report that every potential security incident would must be reported and that any complaint received by Booking should be reported by the Security Team be investigated. As soon as a controller becomes aware of a security incident or has been made aware of a possible infringement by another source, the controller to investigate whether there has been a reportable breach.23 From the “Data Incident Response Policy” shows that Booking has set up its policy in such a way that suspicions of and reports of suspected security incidents should be immediately scaled up for assessment to the security team. The AP is of the opinion that this did not happen in the present case at the expense and risk of Booking. In doing so, the AP once again points to the situation that emerges from the various reports from the accommodations, virtually no other conclusion was possible than that this was the case of a substantial reportable breach.

Obvious error in report

Booking has argued that the investigation report in paragraph 26 erroneously dates February 2, 2019 mentions on which the Security Team of Booking recorded its findings, but that date not mentioned anywhere else in the documents. The AP assumes that this is an apparent clerical error now no clue can be found in the documents for the fact that the Security Team would have presented its findings on February 2, 2019.

Superfluously

Although this is not under discussion in this case, Booking has indicated large in its opinion value data security and immediate action on data breaches. She means generously to meet and even exceed the expectations of Article 34 of the GDPR by data subjects inform about data breaches even when it is unlikely that a major risk to the rights and freedoms of those involved. The AP welcomes such actions, but emphasizes that this is Booking does not relieve you of the other obligations included in the GDPR, such as the ones in Article 33, first paragraph, of the GDPR laid down reporting obligation.

3.4.5 Conclusion

In view of the foregoing, the AP is of the opinion that Booking article 33, first paragraph, of the GDPR from 16 January 2019 through February 6, 2019, as Booking breached the has not reported personal data to the AP in time, without unreasonable delay.

22 See Guidelines p. 14/15.

23 See the WP29 Guidelines on this in detail.

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

4. Fine

4.1 Introduction

Due to the violation established above, the AP uses its authority to to impose a fine on Booking on the basis of Article 58, second paragraph, preamble and under i and Article 83, fourth paragraph, of the GDPR, read in conjunction with Article 14, third paragraph, of the UAVG. The AP uses the Fining Policy Rules 2019 (hereinafter: Fining Policy Rules).24

In the following, the AP will first briefly explain the fine system, followed by the motivation of the fine in the present case.

4.2 Fining Policy Rules of the Dutch Data Protection Authority 2019 (Fining Policy Rules 2019)

Pursuant to Article 58, second paragraph, opening words and under i and Article 83, fourth paragraph, of the GDPR, read in connection with Article 14, third paragraph, of the UAVG, the AP is authorized to notify Booking in the event of a to impose an administrative fine of up to € 10,000,000 in violation of article 33, paragraph 1, of the GDPR, or up to 2% of the total worldwide annual turnover in the previous financial year, whichever is higher.

The AP has established Fining Policy Rules regarding the implementation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.25

Pursuant to Article 2, under 2.1, of the Fining Policy Rules 2019, the provisions regarding violation

of which the AP can impose an administrative fine not exceeding € 10,000,000 or, for

a company, up to 2% of the total worldwide annual turnover in the previous financial year, if this figure

is higher, classified in Annex 1 as Category I, Category II or Category III.

In Appendix 1, Article 33(1) of the GDPR is classified in category III.

Pursuant to Article 2, under 2.3, the AP determines the basic fine for violations classified in category III

within the following fine range: €300,000 and €750,000 and a basic fine of €525,000.

Pursuant to Article 6, the AP determines the amount of the fine by increasing the amount of the basic fine (to

at most the maximum of the bandwidth of the fine category linked to a violation) or

down (to at least the minimum of that bandwidth). The base fine is

increased or decreased depending on the extent to which the factors referred to in Article 7 are used

give rise.

Pursuant to Article 7, without prejudice to Articles 3:4 and 5:46 of the General Administrative Law Act, the AP

24 Stct. 2019, 14586, March 14, 2019.

25 Stct. 2019, 14586, March 14, 2019.

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

(Awb) take into account the factors derived from Article 83, second paragraph, of the GDPR, in the

Policy rules referred to under a to k:

a. the nature, gravity and duration of the breach, taking into account the nature, scope or purpose of the

processing in question as well as the number of data subjects affected and the extent of the harm suffered by them

injury;

b. the intentional or negligent nature of the breach;

c. the measures taken by the controller […] to mitigate the losses suffered by data subjects

limit damage;

d. the extent to which the controller […] is responsible in view of the technical and

organizational measures he has implemented in accordance with Articles 25 and 32 of the GDPR;

e. previous relevant breaches by the controller […];

f. the degree of cooperation with the supervisory authority to remedy the breach and

limit the possible negative consequences thereof;

g. the categories of personal data affected by the breach;

h. the manner in which the supervisory authority became aware of the breach, in particular whether, and

if so, to what extent, the controller […] has notified the breach;

i. compliance with the measures referred to in Article 58, second paragraph, of the GDPR, insofar as they are earlier

in respect of the controller […] in question in relation to the same

matter have been taken;

j. adherence to approved codes of conduct in accordance with Article 40 of the GDPR or of

approved certification mechanisms in accordance with Article 42 of the GDPR; and

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

financial gains made, or losses avoided, which may or may not result directly from the breach

result.

Pursuant to Article 9 of the Fining Policy Rules 2019, the AP, when setting the fine,

taking into account the financial circumstances of the offender. In case of reduced or

insufficient capacity of the offender, the AP can further moderate the fine to be imposed, if,

after application of article 8.1 of the policy rules, determination of a fine within the fine range

of the next lower category would, in its opinion, nevertheless lead to a disproportionately high fine.

4.3 Fine amount

4.3.1. Nature, seriousness and duration of the infringement

Pursuant to Article 7, preamble and under a, of the Fining Policy Rules, the AP takes into account the nature, the

seriousness and duration of the infringement. In assessing this, the AP takes into account, among other things, the nature and

size

or the purpose of the processing as well as the number of data subjects affected and the scope of the processing by them

damages suffered.

The protection of natural persons with regard to the processing of personal data is a fundamental right.

Pursuant to Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16,

Everyone has the right to, paragraph 1 of the Treaty on the Functioning of the European Union (TFEU).

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

protection of his personal data. The principles and rules regarding the protection of

natural persons when processing their personal data must comply with

their fundamental rights and freedoms, in particular their right to protection

personal data. The GDPR aims to contribute to the creation of an area of freedom,

security and justice and of an economic union, as well as to economic and social progress, the

strengthening and convergence of economies within the internal market and the well-being of natural

persons. The processing of personal data must serve people. The right to

protection of personal data is not absolute, but must be considered in relation

to its function in society and must, in accordance with the principle of proportionality, against others

fundamental rights are considered. Any processing of personal data must be fair and lawful

to happen. The personal data must be adequate, relevant and limited to

what is necessary for the purposes for which they are processed. Personal data must be

processed in a manner that ensures appropriate security and confidentiality of that data,

also to prevent unauthorized access to or the unauthorized use of personal data and

the equipment used for processing.

Reporting breaches should be seen as a means of ensuring compliance with related rules
improve the protection of personal data. If a breach related to
personal data takes place or has taken place, this may result in physical, material or
immaterial damage to natural persons or any other economic or social disadvantage
the person in question. Therefore, the controller should, as soon as he becomes aware of
a personal data breach to the supervisory authority without delay and if possible within 72 hours
notify you of the personal data breach. The supervisor is involved in this
to properly perform its tasks and powers, as laid down in the GDPR.
Not only did Booking fail to promptly notify the personal data breach,
but on several occasions, namely on January 9, 13 and 20, 2019, while immediate action had
may be expected, inaction, resulting in a (very) unreasonably delayed notification
the AP. It has also turned out that Booking, instead of making a notification in steps, is consciously doing this
has chosen to first conduct a thorough investigation before making the required report
the supervisory authority. This is not in line with the regulation as laid down in the GDPR.
The investigation conducted by Booking's Security Team has shown that possibly 4109
stakeholders are affected. These were hotel guests, who booked hotel stays via the Booking platform,
at 40 different accommodations. By committing “social
engineering” fraud, in addition to name and address details and data regarding hotel reservations, also credit card
data to unauthorized third parties. This is sensitive data that is in the hands of
unauthorized persons can lead to financial or other disadvantage.
Given the nature of the personal data, the number of personal data, the number of data subjects affected,
the duration of the violation as well as the importance of timely reporting to the supervisor within 72

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

Intentional or negligent nature of the infringement (culpability)

hours, in the opinion of the AP there is a serious violation, but the AP sees none in this case

reason to increase or decrease the basic fine amount.

4.3.2

Pursuant to Section 5:46(2) of the Awb, when imposing an administrative fine, the AP

take into account the extent to which this can be attributed to the offender. Pursuant to Article 7(b)

of the Fining Policy Rules 2019, the AP takes into account the intentional or negligent nature of the infringement.

Article 33, paragraph 1, of the GDPR prescribes that a personal data breach cannot be committed without

unreasonable delay must be reported and, if possible, no later than 72 hours after the

controller has taken note of this. There is a reporting obligation as such in the Netherlands

since 1 January 2016, when this standard was introduced in the Personal Data Protection Act

(Wbp).26

The AP takes a position with regard to the knowledge that a standard addressee, such as Booking in this case, of the

applicable laws and regulations is deemed to have, on the point of view based on te

market parties bear their own responsibility to comply with the law.27

The AP has also provided ample information to market parties about the applicable laws and regulations, so that

it can be assumed that Booking was also aware of this. In addition, in the media extensively

paid attention to the obligation to report data breaches.

From the legal framework set out above in conjunction with the applicable guidelines of the

WP29, which Booking could have become aware of before the infringement, follows in the opinion of the

AP sufficiently clear that Booking should have reported the breach to the AP in time and that this was done without

unreasonable delay, but in any event should have taken place no later than 72 hours after January 13, 2019.

Moreover, the notification to the AP could have been made conditionally, in the sense that the notification

could be added later. This option is expressly provided in the GDPR.

If doubt had arisen about the scope of the commandment, then, also according to settled case law, te

apply that may be obtained from a professional and multinational market party such as Booking

is required to inform itself properly or to be informed about the restrictions to which it is subject

behaviors are subject, so that she could have geared her behavior to the

scope of that commandment.28

In the AP's opinion, it does not exculpate Booking as an independent bearer of rights and obligations

a [CONFIDENTIAL] of Booking has violated Booking's own protocol that

prescribes that any suspicion of an incident be immediately forwarded to the Security Team for assessment.

This is attributable to Booking.

26 In Article 34a, first paragraph, of the Wbp.

27 Cf. CBb 25 June 2013, ECLI:NL:CBB:2013:4, r.o. 2.3, CBb 25 January 2017, ECLI:NL:CBB:2017:14, r.o. 5.2, CBb March 8,

2017,

ECLI:NL:CBB:2017:91, r.o. 6.

28 Cf. CBb 22 February 2012, ECLI:NL:CBB:2012:BV6713, r.o. 4.3, CBb 19 September 2016, ECLI:NL:CBB:2016:290, r.o.

8.6., CBb 19

September 2016, ECLI:NL:CBB:2016:372, r.o. 6.3.

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

Damage mitigation measures

Booking reported 22 days late. The AP considers this culpable. However, the AP sees no reason

to determine the basic amount of the fine under Article 7(b) of the Fining Policy Rules 2019

increase or decrease.

4.3.3

Pursuant to Article 7, under c, of the Fining Policy Rules 2019, the AP takes into account the

measures taken by the controller to mitigate the damage suffered by the data subject

to limit.

Booking has stated in its opinion that it has various concrete remedial actions

taken to limit any damage to those involved. For example, Booking has informed those involved

and advised on taking mitigation measures. Booking has also prepared itself

declares to compensate any damage (suffered or to be suffered) by those involved. Finally has

Booking notified the affected accommodations immediately and alerts on the platform

Booking posted.

The AP is of the opinion that although Booking failed to report the breach in time to the

supervisor, it is to Booking's credit that it has taken the aforementioned measures and is prepared

declared to compensate for any damage. The fact that Booking has ultimately acted energetically on this point

occurred, as a result of which the harmful consequences for those involved are most likely limited

remained, the AP takes into account when determining the fine amount.

In view of the measures taken by Booking in response to the infringement to mitigate the damage

to limit those involved, the AP sees reason to set the basic amount of the fine under Article 7,

under c of the Fining Policy Rules 2019 to be reduced by € 50,000.

4.3.4

Furthermore, the AP sees no reason to increase the basic amount of the fine on the basis of the other provisions in Article 7 of

the

Fining Policy Rules 2019, insofar as applicable in the present case,

to increase or decrease.

The AP sets the fine amount for violation of Article 33, first paragraph, of the AVG in view of the provisions in Article

7 of the GDPR fixed at € 475,000.

4.3.5

Booking has a primary view with regard to the imposition of an administrative fine

argued that imposing an administrative fine would be disproportionate. By Booking is there

referred to fines imposed by the

Lithuanian, Hungarian and Hamburg Authority.29 Booking takes the position that in the context of

View of Booking and response AP

Other circumstances

29 Paragraph 9.2, under a, of the opinion.

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

the idea of harmonization should be equal fines for similar offenses within Europe

imposed.

There are currently no common starting points at European level for the calculation of

agreed fines. As a result, the AP independently applies the set by it

Fining policy rules for the calculation of fine amounts. Moreover, the AP assesses this case on its own merits

own merits and thus to the specific facts and circumstances of this case. It goes without saying

that they differ from case to case and are therefore not comparable. Finally, the booking

fining decisions of other privacy regulators put forward in its opinion

has come through the so-called consistency mechanism, as laid down in Chapter 7 of the GDPR, and is

the AP is thus already not bound by those decisions and not obliged to in the present one

to impose a fine of the same amount.

Booking has also argued that imposing an administrative fine would be contrary to the

lex certa principle, because clear guidelines from the AP and the European Committee for

Data protection for motivating a delayed notification of a data breach is missing.

The AP also does not share this position of Booking and refers to what has been said in paragraphs 3.4.4 and

4.3.2 of this decision has been considered.

Finally, Booking has argued (more) in the alternative that if the AP nevertheless decides to impose a fine lay, this on the basis of article 6 jo. 8.1 of the Penalty Policy Rules should be reduced to the lowest fine in category II.

With regard to the nature, seriousness and duration of the violation, Booking has argued in short that the preventive and corrective measures taken by Booking the number of people affected and the limited the extent of the damage.

Referring to section 4.3.1, the AP sees no reason to refrain from it on this basis imposing an administrative fine or reducing the amount of the fine.

With regard to the intentional or negligent nature of the infringement, Booking has argued that the violation does not follow from any intent or negligence on the part of Booking and refers to the technical and organizational measures taken to prevent social engineering incidents and to limit consequences.

The AP rejects this position. As stated in section 4.3.2, the AP is of the opinion that there is a negligence that can be attributed to Booking. The AP sees no reason in this to increase or decrease the basic fine amount.

With regard to the measures taken to limit the damage, Booking states that the technical and organizational measures it has put in place are appropriate and may even meet the requirements of the GDPR surpass.

As discussed above in section 4.3.3, the AP sees reason for this to reduce the basic fine.

With regard to the degree of responsibility in view of the conditions imposed by Booking on the basis of Articles 25 and

32 of the GDPR, the technical and organizational measures taken by Booking have argued that the
Booking's systems and organization are set up in such a way that the principles of data protection
can be effectively implemented, with Booking reiterating that it is considering the impact
measures and the nature of the incident cannot be held liable for the data breach and the
alleged violation.

The AP does not share this point of view. A professional party such as Booking may, partly in view of the nature and the extent of the processing, it is expected that it fully adheres to the applicable standards
verified and complied with. As previously considered in paragraph 4.3.2 of this decision, Booking is fully
responsible for the violation. That is why the AP sees no reason to fine this either
to lower.

With regard to previous relevant breaches of the GDPR, Booking has argued that it has no previous
has received messages from the AP about alleged violations of Article 33, first paragraph, of the GDPR.
The AP does not see why Booking's position should lead to a reduction in the
basic fine amount. The fact that the AP Booking has not previously written for an identical
violation does not lead to the determination that a reduction of the fine is eligible.

[CONFIDENTIAL]

With regard to the cooperation between Booking and the AP in order to prevent the alleged violation
remedy and limit the possible negative consequences thereof, Booking has argued that it
has fully cooperated with the AP by answering all questions in a timely manner and, if requested by the
AP had asked for a further explanation of the delay in reporting, this explanation would be
datum.

The AP does not see this as a reason to reduce the fine amount. The AP is of the opinion that the
cooperation of Booking has not gone beyond its legal obligation to comply with Article 33,
first paragraph of the GDPR. Booking has not cooperated with the AP in a special way.

With regard to the other factors, Booking has argued in short that the data does not contain any
relate to special categories of personal data or a vulnerable group of persons,

Booking has been fully transparent to those involved and the AP and the data breach has been reported to the AP reported. Finally, Booking argued that if it had made its notification to the AP earlier, this

would not have led to other measures on the part of Booking or further limitation of the risks for the privacy of data subjects. None of those involved suffered any harm by the time of the notification, according to Booking.

The AP does not follow Booking's view in this regard either. Despite the fact that the infringement, as far as we know, has not affected special personal data, Booking has independent data subjects informed and the (financial) consequences for those involved have remained limited, the AP sees through the seriousness of the violation and the culpability of Booking is no reason to further increase the fine to lower. The AP refers to paragraphs 4.3.1 and 4.3.2 for the reasons for this.

4.3.6 Proportionality and statutory maximum fine

Finally, the AP assesses whether the application of its policy for determining the amount of the fine given the circumstances of the specific case, does not lead to a disproportionate outcome. Applying the principle of proportionality means, according to the Fining Policy Rules 2019, that the AP, if necessary, when setting the fine takes into account the financial circumstances of the offender.

In view of all that has been considered above, the AP is of the opinion that the amount of the fine to be imposed is not up to leads to a disproportionate outcome. In addition, the present decision was made through the AGV prescribed coherence mechanism. The other (concerned) supervisors in Europe have endorsed the opinion of the AP.

The AP sees no reason to assume that Booking will be fined €475,000 given its

financial position could not bear.

4.4 Conclusion

The AP sets the total fine amount at € 475,000.

Date

December 10, 2020

Our reference

[CONFIDENTIAL]

5. Operative part

Fine

The AP imposes an administrative fine on Booking for violation of Article 33, first paragraph, of the AVG

in the amount of € 475,000 (in words: four hundred and seventy-five thousand euros).30

Yours faithfully,

Authority for Personal Data,

drs. C.E. Mur

Board member

Remedies Clause

If you do not agree with this decision, you can within six weeks from the date of sending it

decides to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority.

Pursuant to Article 38 of the UAVG, submitting a notice of objection suspends the operation of the

decision to impose the administrative fine.

To submit a digital objection, see www.autoriteitpersoonsgegevens.nl, under the heading Objection

against a decision, at the bottom of the page under the heading Contact with the Dutch Data Protection Authority.

The address for submission on paper is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.

Mention 'Awb objection' on the envelope and put 'bezwaarschrift' in the title of your letter.

Write in your notice of objection at least:

- your name and address;

- the date of your objection;

- the reference referred to in this letter (case number); or enclose a copy of this decision;

- the reason(s) why you disagree with this decision;

- your signature.

30 The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB).