Registered mail

Booking.com B.V.

The board of directors

attn [CONFIDENTIAL]

PO Box 1639

1000 BP Amsterdam

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

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

authority data.nl

Dear [CONFIDENTIAL],

The Dutch Data Protection Authority (AP) has decided to inform Booking.com B.V. (Booking) an administrative 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 because Booking has failed to commit a personal data breach within 72 hours after it was made known, to be reported to the AP.

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. Chapter 4 elaborates on the (level of the) administrative fine and Chapter 5 contains the operative part and the remedies clause.

Annex(es) 1

1

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

1 Introduction

1.1 Relevant legal entities

Booking is a private company with its registered office at Herengracht 597 (1017 CE) te 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 where Trip Providers, such as accommodations, can offer 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 the US NASDAQ Stock Market Listed Booking Holdings Inc. The latter had apparently its 2019 public and consolidated financial statements reported sales of $15.1 billion (EUR 13,727,410,000) and a net income of USD 4.9 billion (EUR 4,454,590,000).

1.2 Reason for research

On February 7, 2019, Booking notified the AP of a personal data breach (data breach) done. An unknown third party had access to a Booking reservation system by pretending to be an employee of Booking at multiple accommodations. Here are the personal data of several involved parties, which via the Booking platform hotel reservations had done, compromised. Because Booking indicated in the notification form that

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

launched an investigation into Booking's compliance with Article 33(1) of the GDPR.

1.3 Process

In a letter dated 12 February 2019, the AP sent an inquiry to Booking. This request is

also sent by e-mail on 26 February 2019.

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

personal data supplemented.

By letter dated 1 March 2019, Booking responded in writing to the request for information of 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 AP sent an additional request for information to Booking.

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

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 informed the other supervisory authorities

authorities on 19 March 2019 of the present case, also finding

that the AP is acting as lead regulator now that Booking's headquarters is located in

The Netherlands.

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

Booking was sent and Booking was given the opportunity to make its point of view known.

Booking has given its opinion on this intention in writing by letter dated 3 September 2019 and

the underlying report.

On October 23, 2020, the AP sent 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(1) of the GDPR, this Regulation applies to all or part of automated processing, as well as to the processing of personal data that are in a file included or intended to be included therein.

Pursuant to Article 3(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 is carried out 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 about 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” means a […] legal person […] that, alone or together with others, has the purpose of and determine the means of processing personal data; […].

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

Date

Dec 10, 2020

Our reference

[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

Under Article 4, twelfth, of the GDPR, a “personal data breach”

means a breach of security that accidentally or unlawfully leads to the destruction,

the loss, alteration, unauthorized disclosure of or access to

transmitted, stored or otherwise processed data.

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

connection with personal data without undue delay and, if possible, no later than 72

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

authority, unless it is not likely that the infringement will pose a risk to the rights and freedoms

of natural persons (…). In the event that 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 of the leading supervisory authority

Pursuant to Article 55(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(1) of the GDPR, the supervisory authority of the principal place of business or the

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

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

controller (…) in accordance with the procedure referred to in Article 60.

3. Review

3.1 Competency AP

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

data subjects in more than one Member State have experienced material consequences.1 This means that cross-border processing within the meaning of Article 4(23)(b) of the GDPR. The AP states establishes that it is competent to act as lead supervisory authority under Article 56 of the GDPR authority now that Booking's head office is located in Amsterdam.

1 See section 3.4.2.

3.2 Processing of personal data

According to Article 4(1) of the GDPR, personal data concerns all 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 them.

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 places to stay and stay overnight search for day trips after which they can be reserved via the platform.

When making a reservation via the Booking platform, personal data such as: contact, reservation and payment details entered. Booking will then provide 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 displayed on the Trip Provider page at Booking.com displayed, including 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 consult necessary reservation details of the guests.

Booking's Security Team engaged in response to the breach has determined that a unknown third party has gained access to the Extranet of Booking. The findings of the Security Team are recorded in a so-called Security Incident Summary report. From it in the file included Security Incident Summary report of 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 283 persons involved the credit card details of which 97 with the 'card verification code'.3

The reported breach in connection with Booking's personal data thus concerns, among other things, names, address details, telephone numbers and credit card details of hotel guests. Now that this concerns information 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 1: notification of a personal data breach 7-2-2019, p3.

3 File 9, Responses from Booking to a request for information, Appendix 5.

The AP has established that personal data is processed via the Extranet: the data are recorded, stored and further disclosed in the Extranet. 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 a controller

as referred to in Article 4(7) of the GDPR. It is important to establish who the purpose 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 through Booking.com and

are then 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

are processed. The Privacy Statement states, among other things, that Booking shares data with third parties,

including the “Travel Provider”, or the Trip Provider. That the data is shared with the travel provider

shared via the Extranet is apparent from, among other things, the notification of the infringement on 7 February 2019 and the

view of Booking.4 The Privacy Statement also explicitly states that the processing of the aforementioned

personal data mentioned is done by Booking (Herengracht 597, 1017 CE Amsterdam,

Netherlands).5

In addition, Booking determines the implementation of the security of the Extranet by taking

security measures for access control such as “two factor authentication” (of which the code

is also generated by Booking).6 Furthermore, in addition to other security measures, Booking has

set up a data breach reporting procedure for incidents concerning the Extranet.7

The AP therefore determines on the basis of the aforementioned that Booking determines the purpose and means for

the processing of personal data relating to reservations made via the platform of

Booking are made, and that via the Extranet (a system used by Booking and

managed) are processed.

In its view, Booking has argued 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 20: research report, marginal 17 et seq., opinion marginal 2.3 et seq.

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

6 Opinion, marginal 2.5.

7 Opinion, marginal numbers 2.6, 3.2 and 3.3.

8 View, marginal 2.2.

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

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

are made available and that Booking is not responsible for

data processing activities of the Trip Providers.9

That Trip Providers can also (physically) process personal data in the Extranet,

without prejudice to the fact that Booking is the data controller for the Extranet. And so too

responsible for what happens with the personal data in the Extranet. The argument of

Booking is therefore not successful.

That Booking also sees itself as a controller for the personal data sent via the

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

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

to be the controller for the customer data processed via its platform.10

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

of Article 4(7) of the GDPR.

3.4 Breach Report Violation

3.4.1 Introduction

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

occurred, the controller without undue delay and, where possible,

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

unless the personal data breach is unlikely to pose a risk

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

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

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

connection with personal data should have reported (timely) to the supervisory authority.

3.4.2 Facts

January 9, 2019

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

[CONFIDENTIAL] from Booking by email that a guest has 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's date of birth or other bank card details

wanted to give up so that a reserved night could be paid in advance. The property manager

asks Booking in his email to investigate the incident now that the property is operating from the

Extranet does not have access to customer e-mail addresses and he thinks that there is likely to be

9 Opinion, marginal number 2.3.

10 View, marginal 2.2.

11 In other words: a Trip Provider.

Date

Dec 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 accommodation.

Email from 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 over. 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 […]"

Attached to the aforementioned e-mail was the e-mail that the data subject had received from the unknown third party receive. It appears from this email that the unknown third party using the reservation details

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

Email of 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 the rate for 1st night is 450 emarati dirhams.

many thanks

[…]

Reservations department”

January 13, 2019

On January 13, 2019, the same accommodation (I) reported to the aforementioned [CONFIDENTIAL] of Booking that a similar complaint has been received from another guest. An unknown party had – this time by telephone – made known to the guest on behalf of Booking, whereby an attempt was made to obtain his/her credit card and obtain personal data.

Email from January 13, 2019 10:18 AM

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

Hi […]

8/27

Date

Dec 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 because he was on the phone approached with the request to provide his credit card information. The property manager indicates the [CONFIDENTIAL] of Booking that given the seriousness of the situation the matter will become

scaled up to headquarters.

January 20, 2019 17:14 e-mail

“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]”

On January 20, 2019, a second accommodation reports to Booking that there is “an” alarming situation with Booking.com reservations”. Several guests who had booked through Booking, were contacted by telephone with the request to provide their credit card details. Also this accommodation asks Booking's [CONFIDENTIAL] to investigate.

January 20, 2019 11:35 AM email

“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

Dec 10, 2020

Our reference

[CONFIDENTIAL]

Thank you,

[…]

[CONFIDENTIAL]"

Booking applies the policy that suspicions and reports of incidents must be immediately reported

forwarded to the Security Team of Booking.12

The [CONFIDENTIAL] of Booking notified by the properties of the

fraudulent acts by an unknown third party have alarmed the Security Team at Booking

January 31, 2019 informed.

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

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

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

2019.13

This investigation by the Security Team has shown that 40 accommodations in the United Arab Emirates

Emirates have been victims of social engineering fraud, whereby the personal data of

possibly 4109 people involved have been compromised. An unknown third party has

Impersonated 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 could

party log in to the Extranet of Booking in which reservation details of guests are included.

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

been. The persons involved were both 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, surname, 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 regarding 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

results of the investigation. All those involved were also informed by Booking on February 4, 2019

brought.14

The Booking Privacy Team determined on February 6, 2019 that there was a data breach that

had to be reported to the AP.

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

13 File 9, Responses from Booking to a request for information, Appendix 5.

14 Notification form and opinion, marginal 4.4 under d.

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

On February 7, 2019, Booking submitted a notification to the AP as referred to in Article 33, first paragraph, of the

AVG.15

3.4.3 Assessment

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

occurred, the controller without undue delay and, where possible,

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

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

assessed whether there has been a personal data breach. Then it should be

assessed whether the infringement poses a risk to the rights and freedoms of natural persons.

A personal data breach

As the AP established in section 3.4.2, an unknown third party has had access to the
Extranet of Booking and thus gained unauthorized access to the data processed by Booking
data relating 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
guests who had booked through Booking's online platform. In doing so, 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 those involved to try and get them on
to defraud credit card details on the basis of improper grounds. Due to the infringement of the
confidentiality of the data there was not only a risk of financial loss but also of
identity theft or any other harm. The AP therefore finds that the infringement related to
personal data posed a risk to the rights and freedoms of natural persons.

Notification to the competent supervisory authority in accordance with Article 55

Section 3.3 establishes that Booking is the controller. In section 3.1, the AP
determined that it is competent under Article 56 of the GDPR to act as a lead
supervisory authority now that Booking's head office is located in Amsterdam. Booking has
reported the breach to the AP on January 7, 2019. Booking has thus notified the in
competent authority in the present case in accordance with Article 55 of the GDPR.

15 File 1, Notification of a personal data breach 7-2-2019. P 5.

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

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

personal data

The Guidelines for the reporting of personal data breaches under Regulation

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

WP29), contain an explanation of the reporting obligation(s) in the GDPR and offer a handle on how to deal with various

types of infringements should be dealt with.

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

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

a controller shall be deemed to have become aware of a breach in connection

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 AP is of the opinion that Booking was aware of the infringement in connection with at least 13 January 2019.

personal data and consider the following to this end.

On January 9, 2019, Booking's [CONFIDENTIAL] received a first signal, via email

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

the person concerned and the Trip Provider had a serious suspicion that a data breach had occurred. The

the person concerned was approached by e-mail on 8 January 2019 by an (unknown) third party who is known

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

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

an overnight stay could be arranged. From the e-mail of 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 caused by (the [CONFIDENTIAL] of) Booking

will be forwarded to Booking's Security Team for further investigation now in the email

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

Booking platform was created. This is 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 appointed by the accommodation manager subject of the email: “[External] Fraud / Leaked Guest Information/ URGENT”. The Security Team had

can start an exploratory investigation.

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

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

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

data subject reservation made via the Booking platform. The property manager has in his e-mail

mail to the [CONFIDENTIAL] of Booking expressly indicated that the incident is equivalent

16 Guidelines for the reporting of personal data breaches under Regulation 2016/679 Working Party

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

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

Booking.com

The AP is of the opinion that Booking is in any case deemed to have knowledge of the on January 13, 2019.

personal data breach, because with the above information, Booking has a reasonable

had assurance that a security incident has occurred leading to the compromise of

personal data processed by Booking. The Trip Provider's Property Manager

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

the Extranet, where personal data of guests was compromised.

Given the alarming situation, Booking should have immediately forwarded the incident to the Security Team of Booking so that an investigation into the extent of the infringement could be carried out, which, however, was Booking until January 31, 2019 has been neglected.

On the basis of the foregoing, the period of 72 . prescribed in Article 33(1) of the GDPR has hours prior to reporting a breach to the AP, commenced on January 13, 2019. As a result Booking should have submitted the personal data breach to the AP by January 16, 2019 report. It has been established that Booking did not make this notification until February 7, 2019, so 22 days late.

This also applies if the date is 20 January 2019, the date on which next to accommodation I is also another Trip Provider (accommodation II) in the United Arab Emirates Emirates has reported similar incidents to the [CONFIDENTIAL] of Booking. Also in this email notification subject is boldly capitalized: **SECURITY BREACH**. In that case, the personal data breach would be 15 days late with the supervisory authority have been reported.

3.4.4 Booking opinion and AP . response

Notification of infringement

In its view, Booking has primarily taken the position that there is no question of a violation as she only became aware of it on February 4, 2019, after completion of the internal investigation of the infringement, after which it is timely and without undue delay within 72 hours of becoming aware reported, which according to Booking is in line with Article 33(1) of the GDPR.

The AP does not follow this position. As can be seen from the foregoing, the AP has established that Booking on 13 became aware of the infringement in January 2019. It follows that Booking has committed the infringement related to has not reported personal data in accordance with the provisions of Article 33(1) of the GDPR.

Notifications accommodations

With regard to the signal from accommodation I on January 9, 2019, Booking has in its view argued that the [CONFIDENTIAL] of Booking had considered at the time that there was no

there was a reason to scale up the report to the Security Team of Booking, because the

the person concerned was approached by e-mail. Booking states that e-mail addresses will be in the Extranet hashed and cannot be extracted from it. Furthermore, Booking argues that the affected accommodation and the [CONFIDENTIAL] of Booking would have come to the conclusion together that “it probably wasn't an incident at Booking”.

With regard to the latter, the AP notes that in addition to the fact that no substantiation has been given for this in the opinion, it is established that the [CONFIDENTIAL] of Booking has not acted in accordance with its own Booking protocol, 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 by Booking to the Security Team. Indeed, the fact that the email in question contained the exact reservation details of the person concerned and the fact that the booking was made through Booking's platform, the [CONFIDENTIAL] of Booking should alarm and move to further action.

With regard to the incident of January 13, 2019, Booking argued that the [CONFIDENTIAL] in issue did not see any direct resemblance to the prior incident, thereby not showing to a reasonable degree assurance 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 had already considered that there was an equivalent incident and that the security incident had to be have with the Extranet, for which Booking is the controller, means that Booking on that knew with a reasonable degree of certainty – and therefore had knowledge – that an infringement had occurred in connection with personal data. Also in this case the exact reservation details were

of the person concerned 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 was compromised. It was highly certain that these data a platform used by Booking for its business activities had been obtained, now as evidenced the e-mail correspondence could be excluded according to the Trip Provider and the persons involved in question that a security incident had occurred on their side.

Violation of internal reporting obligation

Booking has further argued that it cannot be argued against Booking that the procedure for security incident reporting, which means that security incidents are reported by the Trip Providers via 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 opposed. Booking has hereby referred to a decision by the Hungarian privacy regulator, who would have ruled that negligence from only one part of the organization cannot be held against the entire organization if appropriate measures were taken hit.18

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

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

The AP states first and foremost that Booking, as a controller, has an obligation to alarming signal to investigate a possible breach of the security of

personal data, so that action can be taken in a timely manner and in line with the provisions of the GDPR if a personal data breach has occurred. According to the AP, this is independent of 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 submitted by Booking The “Data Incident Response Policy” also shows that all suspicions of incidents, even if they “third party service providers” as the aforementioned Trip Providers have been reported to Booking, must be 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. (…)”.

Various data incidents were reported by the accommodations on January 9, 13 and January 20, 2019. (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 informed of the breach, nevertheless the Security Team is 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 by the same organizational unit (of a government body) and not for a case of “social engineering” where there is a form of fraud, but also that the DPA in that decision has a different opinion of the supervisor reads than is outlined by Booking. The late notification in that case of an infringement as referred to in Article 33(1) of the GDPR because an employee received it too late is continued, contrary to what Booking suggests, the organization in question is indeed Hungarian supervisor accused.

Personal privacy risk

Booking further argued that the investigation report erroneously identified a risk to the personal

privacy has been assumed without making an analysis of the implemented by Booking

security measures aimed at protecting privacy and removing

adverse consequences and mentioned 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 has been advised and Booking has indicated that it will compensate all damage suffered.

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

The AP does not follow Booking's last position. As soon as personal data, as in this case, is

end up in an unauthorized person and have been seen, there is already a risk to the rights

and freedoms of natural persons. This risk has also manifested itself in the present case

now that those involved had been approached by an unknown third party who unlawfully had access to the personal data

of those involved. That Booking subsequently promised to pay any financial damage

compensation does not alter the fact that the personal data has ended up in the wrong hands. It

the risk of possible consequences of the infringement is thus not removed.

Notification within 72 hours

Booking has further argued that making a report within 72 hours as referred to in Article 33,

first paragraph of the GDPR is not always possible. It can weeks specialized security teams or

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 not in accordance with the AVG if the AP would expect Booking in general only three days to get a investigate and become aware of a personal data breach. In addition according to Booking, the WP29 explicitly states in its Guidelines that it may take some time before a controller can determine the extent of the breaches and controller is better able to prepare a meaningful report in which several, strongly similar seeming violations are combined rather than reporting each violation separately. Finally, Booking argued that the investigation report erroneously considers that Booking does not has given a valid reason for the (alleged) violation of the 72-hour period. In the notification of February 7, 2019, clear reasons are given, located in the thorough investigation by Booking, whereby Booking reiterates that it primarily takes the position that the report was made within 72 hours after it became aware of the personal data breach.

The AP considers the following in this regard.

The AP endorses the view 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 necessary information about a breach that enables a report to be made that complies with all requirements laid down in Article 33(3) of the GDPR, the possibility to make a notification has been included in the GDPR in steps. This possibility is provided for in Article 33(4) of the GDPR fixed. 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 paragraph 3.3.3 already noted, Booking must be deemed to have received notice of the . on January 13, 2019 personal data breach. That the infringement pursuant to Article 33(1) of the GDPR should have been reported, was then also clear. Booking took too long in this case waited to make the notification prescribed in Article 33(1) of the GDPR. the thorough research to which Booking refers in no way justifies the delay of the aforementioned (initial) notification, which therefore constitutes an unreasonable delay as referred to in Article 33, first paragraph, of the

GDPR.

16/27

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

Meaningful notification

With regard to what has been argued by Booking with regard to the preparation of a meaningful

report in which several similar infringements are reported together, the AP considers that

the point in the present case is that Booking was already aware of the infringement on 13 January 2019 and

the – whether or not initial – notification should have been made in a timely manner. That there would be several on top of

each other

seeming infringements that, according to Booking, could be packaged in one meaningful report, the AP – having regard to

on what has been considered above in paragraph 3.4.3 – not relevant.

Delayed notification justification

Booking has argued that outside the Guidelines there are no instructions that indicate

what arguments a delayed notification can be justified and that the AP is a new standard

cannot be applied retroactively. In addition, the AP could have asked for the delay

to be explained in more detail.

The AP considers in this regard that there is no question of retroactive application of a new

norm. The regulation included in the GDPR on this point is clear: when there is an infringement in

relating to personal data, it must be completed without undue delay and, if possible, no later than 72

hours after becoming aware of it to the supervisory authority. The Guidelines give to the

opinion of the AP interpretation for compliance with the obligation(s) to report included in the GDPR

of infringements; they can by no means be judged as a new standard. By the way, it is all

time on the path of the controller to make a notification that cannot be made in a timely manner,

provide adequate justification for this.

Practical implications judgment AP

In its view, Booking has also expressed its concerns about the practical implications of

the judgment of the AP in the investigation report.20 The strict explanation referred to therein, according to

Booking implies 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 manner in which and the content thereof – must be

addressed

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 is needed now. Such unreasonable organizational measures, with associated

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

Dec 10, 2020

Our reference

[CONFIDENTIAL]

The AP states first and foremost that the GDPR prescribes the obligations to which Booking in the capacity of

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

responsible party is obliged to take all appropriate and organizational measures to

ensure a coordinated level of security: the ability to detect, detect and detect a breach in a timely manner

addressing and reporting 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 should be reported and that any complaint made to Booking should be addressed by the Security Team are being investigated. Once a controller becomes aware of a security incident or has been notified of a potential infringement by another source, the controller to investigate whether there has been a reporting 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 scaled up immediately for review to the Security Team. That this has not happened in the present case is, in the opinion of the AP at the expense and risk of Booking. In doing so, the AP once again points to the situation that from the various reports of the accommodations, almost no other conclusion was possible than that this was the case of a substantial notifiable breach.

Obvious error in report

Booking has argued that the investigation report in paragraph 26 erroneously stated February 2, 2019 as the date mentions on which the Security Team of Booking recorded its findings, but that date is not mentioned anywhere else in the documents. The AP assumes that this is an apparent writing now no indication 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 further discussed in this case, Booking has indicated in its opinion that value data security and immediate action on data breaches. She thinks amply to meet and even exceed the expectations of Article 34 of the GDPR by data subjects 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 discharge from the other obligations included in the GDPR, such as those referred to in Article 33(1) 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, now that Booking has breached the infringement related to has not reported personal data to the AP in a timely manner, without undue delay.

22 See Guidelines p. 14/15.

23 See in detail the Guidelines of the WP29.

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

4. Fine

4.1 Introduction

Due to the violation established above, the AP uses its power to Booking to impose a fine 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, paragraph 3, of the UAVG. The AP uses the Fines Policy Rules 2019 (hereinafter: Fines 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 Fine Policy Rules of the Dutch Data Protection Authority 2019 (Fining Policy Rules 2019)

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

The AP has established fine policy rules regarding the interpretation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.25

Pursuant to Article 2, under 2.1, of the Fine Policy Rules 2019, the provisions with regard to violation

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

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

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

In Annex 1, Article 33, first paragraph, of the GDPR is classified in category III.

Pursuant to Article 2, under 2.3, the AP sets 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 (up 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 basic fine will be

increased or decreased depending on the extent to which the factors referred to in Article 7 to that end

give rise to.

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

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

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

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

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

Policy rules mentioned under a to k:

the nature, seriousness and duration of the infringement, taking into account the nature, scope or purpose of the infringement

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

injury;

b. the intentional or negligent nature of the infringement;

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

limit damage;

d. the extent to which the controller […] is responsible given the technical and

organizational measures that he has carried out in accordance with Articles 25 and 32 of the GDPR;

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

f. the extent to which there has been cooperation with the supervisory authority to remedy the breach and

limit the possible negative consequences thereof;

g. the categories of personal data to which the breach relates;

h. the manner in which the supervisory authority became aware of the infringement, 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, paragraph 2, of the GDPR, insofar as they are previously

with regard to the controller […] in question with regard 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, arising directly or indirectly from the infringement

result.

Pursuant to Article 9 of the Fine Policy Rules 2019, when determining the fine, the AP will, if necessary,

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

If the offender has insufficient financial capacity, the AP can further mitigate 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, opening words and under a, of the Fine 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, size

or the purpose of the processing as well as the number of data subjects affected and the extent of the processing by them damages suffered.

The protection of natural persons with regard to the processing of personal data is a fundamental right. Under Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16, paragraph 1 of the Treaty on the Functioning of the European Union (TFEU), everyone has the right to

protection of his personal data. The principles and rules concerning the protection of natural persons when processing their personal data must be in accordance with their fundamental rights and freedoms, in particular their right to protection of personal data. The GDPR aims to contribute to the creation of an area of freedom, security and justice and of 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 to its function in society and must conform to the principle of proportionality against other fundamental rights are weighed up. Any processing of personal data must be fair and lawful to happen. The personal data must be sufficient, 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 use of personal data and the equipment used for processing.

Notification of breaches should be seen as a means of ensuring compliance with the related rules

to improve the protection of personal data. If an infringement in connection with
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 for
the person in question. Therefore, as soon as the controller becomes aware of
a breach of personal data the supervisor without delay and if possible within 72 hours
notify the personal data breach. The supervisor is thus
able to properly perform its duties and powers, as laid down in the GDPR.
Not only did Booking fail to promptly report the personal data breach,
but has on several occasions, namely on January 9, 13 and 20, 2019, while having immediate action
may be expected, has been sitting still, resulting in a (very) unreasonably delayed notification at
the AP. It has also become apparent that instead of making a notification in steps, Booking consciously
has chosen to conduct a thorough investigation before making the required report to
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 4109
stakeholders are affected. These were hotel guests, who booked hotel stays via the Booking platform,
at 40 different accommodations, had made reservations. By committing "social"
engineering" fraud are credit card in addition to name and address details and data regarding hotel reservations
data ended up with unauthorized third parties. This is sensitive data that is in the hands of
unauthorized persons can lead to financial or other disadvantage.
Considering 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 a timely notification to the supervisor within 72

Date

Dec 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 in this case the AP does not see any

reason to increase or decrease the basic fine.

4.3.2

Pursuant to Article 5:46, second paragraph, of the Awb, when imposing an administrative fine, the AP

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

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

Article 33(1) of the GDPR prescribes that a personal data breach without

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

controller has taken cognizance of this. The Netherlands has a duty to report as such

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

(Wbp).26

The AP considers the knowledge that a standard addressee, such as Booking in this case, has of the

applicable laws and regulations is deemed to have, on the basis of

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

The AP has also amply informed market parties about the applicable laws and regulations, so that

It can be assumed that Booking was also aware of this. In addition, the media has 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 taken cognizance of before the infringement, follows in the opinion of the

AP sufficiently clear that Booking should have reported the breach to the AP in a timely manner and that without

unreasonable delay, but in any case should have been made within 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 supplemented 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,

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

requires it to be duly informed or to be informed about the restrictions to which it is

behaviors, so that from the outset she could have aligned her behavior with the

scope of that commandment.28

In the opinion of the AP, it does not exculpate Booking as an independent carrier of rights and obligations that

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

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

This is attributable to Booking.

26 In Article 34a(1) of the Wbp.

27 Cf. CBb 25 June 2013, ECLI:NL:CBB:2013:4, r.o. 2.3, CBb January 25, 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 September 19, 2016, ECLI:NL:CBB:2016:290, r.o.

8.6., CBb 19

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

Damage Reduction Measures

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

to pay the basic amount of the fine pursuant to Article 7(b) of the 2019 Fine Policy Rules

increase or decrease.

4.3.3

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

controller has taken measures to prevent the damage suffered by data subjects

to limit.

Booking has put forward in its view that it has various concrete recovery actions

taken to limit any damage to those involved. This is how Booking informed those involved

and advised on taking damage mitigation measures. Furthermore, Booking has prepared itself

declares to compensate any damage suffered or to be suffered by those involved. Finally,

Booking immediately notified affected accommodations and alerts on .'s platform

Booking placed.

The AP believes that although Booking has failed to report the breach to the

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

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

occurred, so that the harmful consequences for those involved are most likely to be limited

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

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

to limit the data subjects involved, the AP sees reason to adjust the basic amount of the fine pursuant to Article 7,

under c of the 2019 Fine Policy Rules by €50,000.

4.3.4

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

the

Circumstances referred to in the Penalty Policy Rules 2019, to the extent applicable in the present case,

to increase or decrease.

The AP sets the fine for violation of Article 33, first paragraph, of the GDPR in view of the

7 of the GDPR fixed at € 475,000.

4.3.5

With regard to the imposition of an administrative fine, Booking has primarily

argued that the imposition of an administrative fine would not be proportionate. By Booking is therewith

referred to fines imposed by the for violations of Article 33(1) of the GDPR

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

View Booking and response AP

Other circumstances

29 Paragraph 9.2, under a, of the opinion.

Date

Dec 10, 2020

Our reference

[CONFIDENTIAL]

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

imposed.

There are currently no common principles for the calculation of

fines agreed. In this way, the AP independently uses the

Fine policies for calculating fines. In addition, the AP assesses this case on its own

its own merits and thus to the specific facts and circumstances of this case. No need to argue

that these are different from case to case and therefore not comparable. Finally, the Booking

fine decisions of other privacy supervisors put forward in its view have not been effected

came via the so-called coherence mechanism, as laid down in chapter 7 of the GDPR, and is

the AP is therefore not bound by those decisions and not obliged to act in the present case

to impose a fine of the same amount.

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

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 view of Booking and refers to what is stated 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 it down pursuant to Article 6 jo. 8.1 of the Fine 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 briefly that the

preventive and corrective actions taken by Booking the number of people affected and the

limited the extent of the damage.

With reference to paragraph 4.3.1, the AP sees no reason to waive the decision on this basis

imposing an administrative fine or reducing the amount of the fine.

As to the intentional or negligent nature of the infringement, Booking has argued that the

violation does not result 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 attributable to Booking. The AP sees no reason in this

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 taken are appropriate and may even meet the requirements of the GDPR

surpass.

As discussed above in section 4.3.3, the AP sees this as a reason to

basic fine.

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

32 of the GDPR, Booking has argued that the technical and organizational measures

Booking systems and organization are designed in such a way that the principles of data protection
can be implemented effectively, with Booking reiterating that in view of the affected
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 view. A professional party such as Booking may, partly in view of the nature and
scope of processing, are expected to comply with the standards applicable to it
verified and comply with it. As previously considered in section 4.3.2 of this decision, Booking is fully
held responsible for the violation. That is why the AP sees no reason to impose the fine
to lower.

With regard to previous relevant breaches of the GDPR, Booking has argued that it has no prior
has received messages from the AP about alleged violations of Article 33(1) of the GDPR.

The AP does not see why this position of Booking should lead to a reduction of the
basic fine amount. The fact that the AP has not previously written to Booking 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
and mitigate its potential negative impact, Booking has argued that it
has fully cooperated with the AP by answering all questions in a timely manner and if the
AP had asked for a further explanation of the delay in reporting, this explanation would be
given.

The AP sees no reason in this to reduce the fine. The AP is of the opinion that the
Booking's cooperation has not gone beyond its legal obligation to comply with Article 33,
first paragraph, of the GDPR. Booking has therefore not cooperated with the AP in a special way.

With regard to the other factors, Booking has argued briefly that the data does not
relate to special categories of personal data or a vulnerable group of persons,
Booking has been completely transparent to those involved and the AP and has the data breach itself at the AP

reported. Finally, Booking argued that if it had made its report to the AP earlier, this

would not have led to other measures on the part of Booking or further mitigation of the risks to the privacy of those involved. No person involved has suffered any disadvantage by the time of the notification, according to Booking.

The AP does not follow Booking's view in this either. Despite the fact that the infringement, to the extent that we know, has not affected any special personal data, Booking has independently involved parties informed and the (financial) consequences for those involved have been limited, the AP sees due to the seriousness of the violation and the culpability of Booking no reason to continue 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, on the basis of Articles 3:4 and 5:46 of the Awb (principle of proportionality), the AP assesses whether the applying 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 According to the 2019 Fine Policy Rules, the AP entails that, if necessary, when determining 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 does not exceed leads to a disproportionate outcome. In addition, the present decision was reached through the AGV prescribed coherence mechanism. The other (involved) regulators in Europe have endorsed the judgment of the AP.

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

financial position could not bear.

4.4 Conclusion

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

Date

Dec 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 GDPR

amounting to € 475,000 (in words: four hundred and seventy-five thousand euros).30

Yours faithfully,

Authority Personal Data,

drs. C.E. Mur

board member

Remedies Clause

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

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

In accordance with 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 Den Haag.

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

In your notice of objection, write at least:

- your name and address;

- the date of your notice of objection;

- the reference mentioned in this letter (case number); or attach a copy of this decision;

- the reason(s) why you do not agree with this decision;

- your signature.

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