AUTORITEIT
PERSOONSGEGEVENS

Dutch Data Protection Authority
PO Box 93374, 2509 AJ The Hague
Bezuidenhoutseweg 30, 2594 AV The Hague
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

[redacted]

Date
10 December 2020

Our reference
[redacted]

Contact person
[redacted]

Subject
Decision to impose an administrative fine

Dear [redacted],

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) (hereinafter: the AP) has decided to impose an **administrative fine** of **€ 475,000** on [redacted] (hereinafter: [redacted]). The AP considers that [redacted] infringed Article 33(1) of the General Data Protection Regulation (*Algemene Verordening Gegevensbescherming*) (hereinafter: GDPR)
from 16 January 2019 to 6 February 2019, because [redacted] failed to notify the AP of a personal data breach within 72 hours of becoming aware of it.

This decision is explained in more detail below. Section 1 contains an introduction and Section 2 describes the legal framework. In Section 3, the AP assesses its authority, the processing responsibility and the infringement. Section 4 elaborates on the level of the administrative fine and Section 5 contains the operative part and the remedy clause.

Date
10 December 2020

Our reference
[redacted]

1. Introduction

1.1 Legal entities concerned

[redacted] is a private limited liability company with its registered office at [redacted]. [redacted] was incorporated on [redacted] and entered in the register of the Chamber of Commerce under number [redacted]. [redacted] provides an online platform through which [redacted], such as accommodations, can offer their products and services and users of the platform can then reserve these products and services.
[redacted] is, through various Dutch and English legal entities, an indirect 100% subsidiary of [redacted]., which is listed on the American NASDAQ Stock Market. In 2019, [redacted] had a sales volume of USD 15.1 billion (EUR 13,727,410,000) and a net result of USD 4.9 billion (EUR 4,454,590,000) according to its public and consolidated financial statements.

1.2 Reason for this investigation

On 7 February 2019, [redacted] reported a personal data breach to the AP. An unknown third party had gained access to a reservation system of [redacted] by pretending to be an employee of [redacted] to various accommodations. As a result, the personal data of various data subjects who had made hotel reservations via the [redacted] platform were compromised. Because [redacted] indicated on the notification form that it had discovered the personal data breach on 10 January 2019, the AP commenced an investigation into [redacted]'s compliance with Article 33(1) of the GDPR.

1.3 Course of the investigation

By letter dated 12 February 2019, the AP sent a request for information to [redacted]. This request was also sent by e-mail dated 26 February 2019.

On 27 February 2019, [redacted] provided substantive information in connection with the aforementioned personal data breach notification.

By letter dated 1 March 2019, [redacted] responded in writing to the request for information of 12 February 2019.

By letter dated 6 March 2019, the AP sent an additional request for information to [redacted].

By letter dated 13 March 2010, [redacted] responded in writing to the request for information of 6 March 2019.

By e-mail dated 19 March 2019, the AP sent an additional request for information to [redacted].

Date
10 December 2020

Our reference
[redacted]

By e-mail dated 19 March 2019, [redacted] sent the requested information and an additional document to the AP.

Due to the cross-border nature of the case, the AP informed the other supervisory authorities of the case on 19 March 2019, informing them that the AP would act as lead authority since the head office of [redacted] is located in the Netherlands.

By letter dated 16 July 2019, the AP informed [redacted] of its enforcement intention and provided it with the investigation report, thereby giving [redacted] the opportunity to express its views. By letter dated 3 September 2019, [redacted] expressed its views in writing with regard to this intention and the report on which it is based.

On 23 October 2020, the AP submitted a draft decision to the relevant supervisory authorities in conformity with Article 60 of the GDPR. No objections to this decision have been received.

2.Legal framework

2.1 Scope of the GDPR

Pursuant to Article 2(1) of the GDPR, this decision applies to the processing of personal data wholly or partly by automatic means and to the processing of personal data which form part of a filing system or are intended to form part of a filing system.

Pursuant to Article 3(1) of the GDPR, this decision 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, regardless of whether the processing takes place in the Union or not.

In this decision, pursuant to Article 4 of the GDPR, the following terms have the following meanings:
1. "Personal data": any information relating to an identified or identifiable natural person (data subject); [...].
2. "Processing": any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automatic means [...].
7. "Controller": the [...] legal person [...] which, alone or jointly with others, determines the purposes and means of the processing of personal data; [...].
12. "Personal data breach": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
23. "Cross-border processing": [...] b) processing of personal data which takes place in the context of the activities of a single establishment of a controller [...], but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

2.2 Notification of a personal data breach

Pursuant to Article 4(12) of the GDPR, a "personal data breach" means: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Pursuant to Article 33(1) of the GDPR, a controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (...). If the notification to the supervisory authority is not made within 72 hours, it must be accompanied by the reasons for the delay.

2.3 Competence of the lead supervisory authority

Pursuant to Article 55(1) of the GDPR, each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

Pursuant to Article 56(1) of the GDPR, and without prejudice to Article 55, the supervisory authority of the main establishment or of the sole establishment of the controller (...) shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller (...) in accordance with the procedure provided in Article 60.

3. Assessment

3.1 Competence of the AP

In this case, the processing of personal data by [redacted] had a significant impact on data subjects in more than one Member State.[1] This constitutes cross-border processing within the meaning of Article 4(23)(b) of the GDPR. Since [redacted]'s main establishment is in [redacted], the AP determines that it is competent to act as the lead supervisory authority in accordance with Article 56 of the GDPR.

3.2 Processing of personal data

According to Article 4(1) of the GDPR, personal data means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to one or more factors specific to the physical or physiological identity of that natural person.

[1] See paragraph 3.4.2.

Article 4(2) of the GDPR defines the concept of processing as any operation or set of operations performed on personal data, such as the collection, recording, storage, retrieval, consultation or use of such data.

[redacted] offers an online booking platform through which [redacted], such as accommodation providers and other providers, can offer accommodation, flights, rental cars and day trips to users. Through the platform, users can search for and make reservations for accommodation and day trips. When making a reservation through the [redacted] platform, a data subject enters personal details such as his/her contact, reservation and payment details. [redacted] then provides the details of this reservation to the [redacted] via [redacted] Extranet. [2] [redacted]'s Extranet is an online administrative dashboard with secure access. In addition to access to reservation details in the Extranet, [redacted] have access to all information displayed on the [redacted] page at [redacted], including payment options and policies. To gain access to the Extranet, a [redacted] must enter a username, password and a two-factor authentication pin code. When it has logged on to the [redacted], a [redacted] can consult the necessary reservation details of the guests.

[redacted] called in its Security Team in response to the breach, which found that an unknown third party had gained access to [redacted]'s Extranet. The findings of the Security Team have been recorded in a Security Incident Summary report. The Security Incident Summary report dated 28 February 2019, which is included in the file, shows that the following details of guests that were stored in the Extranet were compromised: first name, surname, address, telephone number, check-in and check-out date, total price, reservation number, price per night, any correspondence between the accommodation and the guest and, with regard to 283 data subjects, their credit card details including the card verification code of 97 of these data subjects.[3]

The reported breach of personal data by [redacted] therefore includes names, addresses, telephone numbers and credit card details of hotel guests. As this concerns information on identified or identifiable natural persons, the aforementioned data can be considered as personal data as defined in Article 4(1) of the GDPR.

The AP has determined that personal data is processed through the Extranet: these data are recorded, stored and further accessed through the Extranet. All the processing on the Extranet constitutes the processing of personal data as defined in Article 4(2) of the GDPR.

3.3 Controller

In the context of the question of who can be held responsible for an infringement of the GDPR, it is necessary to determine who can be considered as the controller as defined in Article 4(7) of the GDPR. It is important to ascertain who determines the purpose and means of processing personal data, which in this case is the processing of personal data of data subjects using the [redacted] platform.

[2] File document 1: notification of a personal data breach 7-2-2019, p3.
[3] File document 9, [redacted]'s replies to requests for information, Appendix 5.

Date
10 December 2020

Our reference
[redacted]

The AP is of the opinion that [redacted] determines the purpose and means of processing personal data relating to reservations made via [redacted].com and then processed via [redacted]'s Extranet. The AP explains this as follows.

[redacted]'s Privacy Statement, as posted on its website, details the personal data processed by [redacted] and the reasons why and the manner in which these data are processed. The Privacy Statement mentions that [redacted] shares data with third parties, including the [redacted]. The fact that the data is shared with the [redacted] via the Extranet is demonstrated by [redacted]'s notification of the breach on 7 February 2019 and the views expressed by [redacted].[4] The Privacy Statement also explicitly states that the processing of the aforementioned personal data is performed by [redacted] ([redacted], the Netherlands).[5]

In addition, [redacted] implements security for the Extranet by taking security measures for access control such as the two factor authentication, the code for which is also generated by [redacted].[6] In addition to other security measures, [redacted] has set up a data breach notification procedure for incidents involving the Extranet.[7]

On the basis of the above, the AP therefore ascertains that [redacted] determines the purpose and means of the processing of personal data relating to reservations made through [redacted]'s platform and processed via the Extranet (a system used and managed by [redacted]).

On the one hand, [redacted] has argued that it is the controller with regard to customer data processed in connection with its platform.[8] On the other hand, [redacted] states that [redacted] act as the controller for the customer data made available through the Extranet and that [redacted] does not consider itself responsible for data processing activities of [redacted].[9]

The fact that [redacted] can also (physically) process personal data on the Extranet, does not alter the fact that [redacted] is responsible for the processing of personal data on the Extranet. This means that it is also responsible for what happens to the personal data on the Extranet. [redacted]'s argument is therefore unfounded.
The fact that [redacted] also sees itself as the processor of personal data processed through the Extranet is also demonstrated by the fact that [redacted] notified the AP of the personal data breach on 7 February 2019 and that [redacted] expresses in its views that it is the controller in respect of customer data processed through its platform.[10]

[4] File document 20: investigation report, marginal 17 ff., views expressed in marginal 2.3 ff.
[5] Under the heading 'Who is responsible for the processing personal data on the [redacted] and how to reach us'.
[6] Views expressed, marginal 2.5.
[7] Views expressed, marginals 2.6, 3.2 and 3.3.
[8] Views expressed, marginal 2.2.
[9] Views expressed, marginal 2.3.
[10] Views expressed, marginal 2.2.

On the basis of the above, the AP ascertains that [redacted] is the controller within the meaning of Article 4(7) of the GDPR.

3.4 Infringement of breach notification obligation

3.4.1 Introduction

Article 33(1) of the GDPR provides that in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent (...), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it must be accompanied by the reasons for the delay.

In this section, the AP will first outline the facts and then assess whether [redacted] should have reported the personal data breach to the supervisory authority in a timely manner.

3.4.2 The facts

9 January 2019
On 9 January 2019, an [redacted][11](I) in the United Arab Emirates informed a [redacted] by e-mail that a guest had complained that they had been contacted by an unknown party posing as an employee of the accommodation with a report that their credit card was not working and whether the guest wanted to provide his date of birth or other bank card details so that a reserved overnight stay could be paid for. In his e-mail message to [redacted], the accommodation manager asked [redacted] to investigate the incident since the accommodation does not have access to customers' e-mail addresses via the Extranet and he thinks that there is probably a data breach at [redacted] because the unknown party was aware of the reservation made at the accommodation through [redacted]'s platform.

E-mail of 9 January 2019 18:00 hours
"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 '[redacted]' 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 [redacted] 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 '[redacted]' email to us. As we do not get guest email address from the extranet, the issue here is likely to be from [redacted]. We don't know how this '[redacted]' managed to get hold of the guest email and that he had made a booking at our property from [redacted]. 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 [redacted].

Kind Regards [...]"

[11] In other words: a [redacted].

Date
10 December 2020

Our reference
[redacted]

The e-mail that the data subject received from the unknown third party was attached to this e-mail. It appears from this e-mail that the unknown third party was trying to obtain personal and/or payment details using the reservation details of the data subject.

E-mail of 8 January 2019 22:32 hours
"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"

13 January 2019
On 13 January 2019, the same accommodation (I) informed the abovementioned [redacted] that the same type of complaint has been received from another guest. An unknown party had made itself known to the guest - this time by telephone - on behalf of [redacted], trying to obtain his credit card and personal details.

E-mail of 13 January 2019 10:18 hours
"Subject: RE: [External Fraud] / Leaked Guest Information / URGENT
Hi [...]
We receive a complaint from another guest...this time someone claiming to be from [redacted] (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 [redacted] instead.
We had taken precautions by changing all our logins (for those who has access) last week Thursday.
Booking no. [...]

Regards
[redacted]

20 January 2019
On 20 January 2019, accommodation I reported that a third guest had complained that he had been contacted by telephone asking for his credit card details to be passed on. The accommodation manager informed [redacted]'s [redacted] that, given the seriousness of the situation, the issue will be forwarded to the head office.

E-mail of 20 January 2019 17:14 hours
"Subject: RE: [External] Fraud / Leaked Guest Information /URGENT

Date
10 December 2020

Our reference
[redacted]

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

Kind regards,
[...] [redacted]

Also on 20 January 2019, a second accommodation reported to [redacted] that there is "an alarming situation with [redacted] reservations". Several guests who had booked through [redacted] were contacted by telephone with the request to provide their credit card details. This accommodation also asked the [redacted] to investigate.

E-mail of 20 January 2019 11:35 hours
"Good morning [...]
We have an alarming situation with [redacted] *reservations. The last couple of days, we have guests reserved through* [redacted]*, 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 [redacted] *password as well as my own password.*

Can you please look into this?

Thank you,
[...]
[redacted]

It is [redacted]'s policy that suspicions and reports of incidents must be forwarded immediately to [redacted]'s Security Team.[12]
[redacted]'s [redacted] who had been informed by the accommodations of fraudulent acts by an unknown third party informed [redacted]'s Security Team on 31 January 2019.
On 4 February 2019, [redacted]'s Security Team completed its initial investigation and concluded that [redacted]'s Privacy Team should be informed. The findings of the investigation by the Security Team are recorded in the aforementioned Security Incident Summary Report dated 28 February 2019.[13]

This investigation by the Security Team revealed that 40 accommodations in the United Arab Emirates had been the victim of social engineering fraud, whereby the personal data of 4,109 data subjects may have been compromised. An unknown third party pretended to be an employee of [redacted] on the telephone in order to obtain the username, password and two-factor authentication code (2FA) of the accommodation.

[12] See file document 15, Reply to request for information with regard to internal policy documents on data breaches.
[13] File document 9, [redacted]'s replies to requests for information, Appendix 5.

This information allowed the third party to log onto [redacted]'s Extranet which contains reservation details of guests. The Security Team has determined that the starting date of the security incident was 19 December 2018. The data subjects were from Europe (including the United Kingdom, 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 the accommodation and, with regard to 283 data subjects, their guest and credit card details including the card verification code of 97 of these data subjects.

On 4 February 2019, the Security Team informed [redacted]'s Privacy Team of the outcome of the investigation. On 4 February 2019, [redacted] also informed all data subjects.[14]

On 6 February 2019, [redacted]'s Privacy Team determined that there was a personal data breach that must be reported to the AP.

On 7 February 2019, [redacted] notified the AP of a personal data breach as defined in Article 33(1) of the GDPR.[15]

3.4.3 Assessment

Article 33(1) of the GDPR provides that in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent (...), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Before the notification is made, therefore, the controller must first assess whether there is a personal data breach. It must then be assessed whether the infringement poses a risk to the rights and freedoms of natural persons.

A personal data breach

As ascertained by the AP in paragraph 3.4.2, an unknown third party accessed [redacted]'s Extranet and thereby gained unauthorised access to the data processed by [redacted] concerning reservations of guests at accommodations. [redacted] also does not dispute the existence of a personal data breach. As a result, the AP ascertains that there is a personal data breach as defined in Article 4(12) of the GDPR.

Risk to the rights and freedoms of natural persons

Following the unauthorised acquisition of the aforementioned personal data, the unknown third party then attempted to use this personal data to obtain credit card details of guests who had booked via [redacted]'s online platform. As a result, the AP not only ascertains that the personal data breach is likely to

[14] Notification form and views expressed, marginal 4.4(d).
[15] File document 1: notification of a personal data breach 7-2-2019, p 5.

jeopardise the rights and freedoms of natural persons, but also that this risk has materialised since the unknown third party contacted many, if not hundreds, of data subjects to try to swindle credit card data on improper grounds. As a result of the confidentiality breach of personal data, there was a risk not only of financial damage but also of identity fraud or any other harm. The AP therefore ascertains that the personal data breach posed a risk to the rights and freedoms of natural persons.

Notification to the competent supervisory authority in accordance with Article 55
In paragraph 3.3 it is established that [redacted] is the controller. In paragraph 3.1, the AP established that it is competent to act as the lead supervisory authority, in accordance with Article 56 of the GDPR, since [redacted]'s main establishment is in Amsterdam. [redacted] notified the AP of the breach on 7 January 2019. In doing so, [redacted] made the notification to the competent authority in this case, in accordance with Article 55 of the GDPR.

Notification not later than 72 hours after the controller becomes aware of a personal data breach
The Guidelines on Personal Data Breach Notification under Regulation 2016/679[16] (hereinafter: Guidelines), drawn up by the Article 29 Data Protection Working Party (hereinafter: WP29), explain the notification requirements of the GDPR and provide guidance on how to proceed in the event of various types of breaches.

The precise moment when a controller can be considered to be aware of a particular breach depends on the circumstances of the particular breach. According to the WP29, a controller should be deemed to have become aware of a personal data breach when it has a reasonable degree of certainty that a security incident has occurred which has led to personal data being compromised.

In the opinion of the AP, [redacted] was aware of the personal data breach in any case on 13 January 2019 and finds as follows.

On 9 January 2019, [redacted]'s [redacted] received an initial signal, via an e-mail from a [redacted] in the United Arab Emirates (accommodation I), that both the data subject and the [redacted] suspected there had been a personal data breach . The data subject was contacted by e-mail on 8 January 2019 by an unknown third party who was familiar with the reservation made through [redacted]'s platform and who, on the basis of this reservation information, was trying to obtain additional personal details in order to supposedly arrange payment for an overnight stay. The e-mail of 8 January 2019, which is included in the file, also attached a PDF document with the booking details. Incidentally, this PDF file has not been submitted by [redacted] and has therefore not been included in the file.

In the opinion of the AP, the aforementioned incident should have been forwarded by (the [redacted] of) [redacted] to its Security Team for further investigation since the e-mail in question contained the precise booking details of the data subject and it had also been established that the booking had been made via [redacted]'s platform. This is even more applicable as the [redacted] had already come to the conclusion

[16] Guidelines on Personal Data Breach Notification under Regulation 2016/679, Article 29 Data Protection Working Party, last revised and adopted on 6 February 2018, 18/NL WP250rev.01.

that there was a security incident and had already made an initial assessment on the basis of the information at his disposal. This is also evident from the subject of the e-mail mentioned by the accommodation manager: "[External] Fraud / Leaked Guest Information / URGENT". The Security Team could have started an exploratory investigation at this time.
On 13 January 2019, (the same [redacted] of) [redacted] received a second message from the aforementioned [redacted]. The data subject in question had been asked for his personal details by telephone by someone posing as an employee of [redacted] who was aware of the reservation made by the data subject through the [redacted] platform. In his e-mail to [redacted]'s [redacted], the accommodation manager expressly stated that he considered the incident to be equivalent to the previous incident and again believed that there must be a data breach on [redacted]'s side.

The AP is of the opinion that [redacted] is deemed to have knowledge of the personal data breach at least on 13 January 2019, because the above information gave [redacted] a reasonable degree of certainty that a security incident had occurred that had led to personal data processed by [redacted] being compromised. In fact, the accommodation manager of the [redacted] had already concluded that there must had been a security incident involving the Extranet whereby personal data of guests had been compromised.

Given the alarming situation, [redacted] should have immediately referred the incident to [redacted]'s Security Team so that the extent of the breach could be investigated, but instead [redacted] failed to do so until 31 January 2019.

On the basis of the above, the deadline of 72 hours for reporting a breach to the AP, as stipulated in Article 33(1) of the GDPR, started on 13 January 2019. As a result, [redacted] should have notified the AP of the personal data breach by 16 January 2019 at the latest. It is an established fact that [redacted] only made this notification on 7 February 2019, i.e. 22 days too late.

The same applies if 20 January 2019 should be adopted as the starting date, which is the date on which another [redacted] (accommodation II) in the United Arab Emirates reported similar incidents to [redacted]'s [redacted] as accommodation I. In this e-mail, the subject is also highlighted in capital letters: **SECURITY BREACH**. In this case, the personal data breach would have been notified to the supervisory authority 15 days too late.

3.4.4 Views expressed by [redacted] and response of the AP

Breach notification
[redacted] has primarily argued in its views that no infringement occurred since it only became aware of the breach on 4 February 2019 upon completion of its internal investigation, after which the breach was notified in a timely manner and without undue delay within 72 hours of [redacted] becoming aware of it. This, according to [redacted], is in conformity with Article 33(1) of the GDPR.

The AP does not agree with this viewpoint. As can be seen from the above, the AP has established that [redacted] became aware of the breach on 13 January 2019. It follows from this that [redacted] did not notify the personal data breach in accordance with the provisions of Article 33(1) of the GDPR.

Reports by accommodations
With regard to the message from accommodation I on 9 January 2019, [redacted] argued when expressing its views that at the time [redacted]'s [redacted] considered that there was no reason to forward the report to [redacted]'s Security Team, because the data subject in question had been contacted by e-mail. [redacted] states that e-mail addresses in the Extranet are hashed and cannot be extracted. [redacted] further argues that the accommodation in question and [redacted]'s [redacted] jointly concluded that "it was probably not an incident at [redacted]".

With regard to the latter, the AP notes that, in addition to the fact that the views expressed by [redacted] do not substantiate this, it is established that [redacted]'s [redacted] did not act in accordance with [redacted]'s own protocol, which stipulates that any suspicion of an incident must be immediately forwarded to [redacted]'s Security Team. The AP is of the opinion that, despite the fact that e-mail addresses are hashed in the Extranet, the aforementioned incident should have been forwarded by [redacted] to the Security Team. After all, the fact that the e-mail in question contained the exact booking details of the data subject and the fact that the booking was made via [redacted]'s platform should have alerted [redacted]'s [redacted] and prompted him to take further action.

With regard to the incident of 13 January 2019, [redacted] argued that the [redacted] in question did not see any direct similarities with the previous incident, which meant that it could not be established with a reasonable degree of certainty that a security incident had occurred at [redacted].

However, the AP is of the opinion that the fact that the (accommodation manager of the) [redacted] had already considered that there was an equivalent incident and that the security incident must be in relation to the Extranet, for which [redacted] is the controller, means that at that time [redacted] did know with a reasonable degree of certainty - and therefore had become aware - that a personal data breach had occurred. Again in this case the precise booking details of the data subject were known to an unknown third party who falsely pretended to be an employee of [redacted]. At this point, [redacted] had a reasonable degree of certainty with regard to the security incident in which personal data had been compromised. There was a high degree of certainty that this data had been obtained from a platform used by [redacted] for its business purposes, since the e-mail correspondence showed that both the [redacted] and the data subject in question could rule out the possibility that a security incident had occurred on their side.

Breach of internal reporting obligation
[redacted] has further argued that the fact that the procedure for reporting security incidents, where security incidents must be reported by the [redacted] to the [redacted] Security Team via the Partner Portal, was infringed by the accommodation in question[17]. According to [redacted], the breach of that obligation to notify and the fact that [redacted]'s [redacted] did not immediately forward the incident should not be

[17] In this case, the accommodation in the United Arab Emirates.

held against [redacted] as a company. [redacted] also referred to a decision of the Hungarian privacy supervisory authority, which found that negligence on the part of only one part of an organisation could not be invoked against the whole organisation if appropriate measures had been taken.[18]

The AP states that it is of paramount importance that [redacted], as the controller, has an obligation to investigate any possible personal data security breach in response to every alarming signal in order to act in a timely manner and in accordance with the provisions of the GDPR. According to the AP, this is separate from any private law agreements that [redacted] may have made in that respect with a third party, such as, in the present case, the [redacted] in question. Paragraph 5.1 of the 'Data Incident Response Policy' submitted by [redacted] also shows that all suspicions of incidents, even if reported to [redacted] by third party service providers such as [redacted], must be immediately forwarded to [redacted]'s Security Team:

> *"Prompt Reporting*
> *All (suspected) Data Incidents must immediately be reported to the [redacted] security team ("Security"). This includes Data Incidents notified to [redacted] from any third party service providers or business partners or other individuals. (...)".*

Although various data incidents were reported by the accommodations to the [redacted] of [redacted] on 9, 13 and 20 January 2019, this did not lead to the required reporting of these incidents to the Security Team, as set out in [redacted]'s own procedures. While [redacted]'s [redacted] was already aware of the breach on 13 January 2019, the Security Team was only informed on 31 January 2019.

Insofar as [redacted] has sought to rely on the principle of equality by referring to the decision of the Hungarian supervisory authority, the AP notes that the case in question is not only a breach of an entirely different nature, namely a breach of the confidentiality of personal data by the same organisational unit (of a public body) and not a case of social engineering involving a form of fraud, but also that the AP understands this decision of the supervisory authority differently than as outlined by [redacted]. The fact that the notification of a breach, as defined in Article 33(1) of the GDPR, was too late in that case because an employee forwarded it too late, was held against the organisation in question by the Hungarian supervisory authority, contrary to what [redacted] suggests.

Risk to privacy

[redacted] also argued that the investigation report wrongly assumed that there was a risk to privacy without analysing the security measures implemented by [redacted] with a view to protecting privacy and removing adverse consequences, and gave a number of examples.[19]

[18] Fining Decision of the Hungarian National Authority for Data Protection and Freedom of Information dated 21 May 2019, NAIH/2019/3854.

[19] The examples mentioned: if a data breach occurs, this is generally limited to contact details, without e-mail addresses, and reservation dates; credit card details are stored in accordance with PCI DSS standards; customers are informed about social engineering and other forms of fraud; the data subjects were immediately informed and given advice after the data breach was detected and [redacted] has indicated that it will compensate all damage suffered.

The AP does not agree with the latter viewpoint of [redacted]. At such time as personal data are in the hands of and are accessed by an unauthorised person, as in this case, then there is already a risk to the rights and freedoms of natural persons. This risk has also manifested itself in this case, where data subjects were approached by an unknown third party who unlawfully possessed the personal data of the data subjects. The fact that [redacted] subsequently undertook to provide compensation for any financial damage does not alter the fact that the personal data ended up in the wrong hands. This does not eliminate the risk of any consequences of the breach.

Notification within 72 hours

[redacted] has also argued that it is not always possible to make a notification within 72 hours, as referred to in Article 33(1) of the GDPR. It can take weeks or months for specialist security teams to connect data points and reach the conclusion that a factual pattern is indeed a data breach that should be notified. Furthermore, it would be wrong and inconsistent with the GDPR for the AP to expect [redacted] to generally only need three days to conduct an investigation and become aware of a personal data breach. In addition, according to [redacted], the WP29 explicitly mentions in its Guidelines that it may take some time for a controller to establish the extent of the breaches and be able to prepare a meaningful notification combining several very similar breaches rather than reporting each breach separately. Finally, [redacted] argued that the investigation report wrongly concluded that [redacted] had failed to give a valid reason for the (alleged) infringement of the 72-hour deadline. The notification of 7 February 2019 gives clear reasons, based on [redacted]'s in-depth investigation, reiterating that [redacted]'s primary position is that the notification was made within 72 hours of it becoming aware of the personal data breach.

The AP considers as follows in this regard.
The AP agrees with the view that an investigation into the scope and precise merits of a breach can take longer than 72 hours. As it is not always possible to have all the necessary information about a breach in order to make a notification that meets all the requirements laid down in Article 33(3) of the GDPR, the option of making a notification in phases has been included in the GDPR. This option is laid down in Article 33(4) of the GDPR. The notification of the breach, however, must take place within the statutory deadline of 72 hours, in accordance with Article 33(1) of the GDPR. As noted in paragraph 3.3.3, it must be considered that [redacted] became aware of the personal data breach on 13 January 2019. The fact that the breach should have been notified, in accordance with Article 33(1) of the GDPR, was also clear at that time. In this case, [redacted] waited too long before making the notification required by Article 33(1) of the GDPR. The thorough investigation to which [redacted] refers in no way justifies the delay of the aforementioned (initial) notification, which therefore constitutes an unreasonable delay within the meaning of Article 33(1) of the GDPR.

Meaningful notification

With regard to the allegations made by [redacted] concerning the preparation of a meaningful notification combining several similar breaches, the AP considers that the issue at stake in the present case is that [redacted] was aware of the breach as early as 13 January 2019 and should have made the notification - initial or otherwise - in a timely manner. The AP does not consider it relevant - in view of what has been considered in paragraph 3.4.3 above - that there are several similar breaches here which, according to [redacted], could be packaged into a single meaningful notification.

Justification of the delayed notification

[redacted] has argued that there are no instructions that specify the arguments for justifying a delayed notification except the Guidelines and that the AP cannot apply a new standard retroactively. In addition, the AP could have asked for a clarification of the delay.

The AP considers that there is no question of applying a new standard retroactively. The rules set out in the GDPR are clear on this point: in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority. The Guidelines, in the opinion of the AP, provide guidance on how to comply with the obligation to notify breaches as laid down in the GDPR and cannot therefore be considered as a new standard. For that matter, it is at all times up to the controller to provide adequate reasoning for a notification that cannot be made in a timely manner.

Practical implications of the opinion of the AP

In the views expressed by [redacted], it also stated its concerns about the practical implications of the opinion of the AP in the investigation report.[20] According to [redacted], the strict interpretation contained therein means that all potential security incidents where there is a risk of personal data being compromised must be reported within 72 hours and that the Security Team must investigate any complaint received by [redacted], irrespective of the manner and content of the complaint. This would impose an unreasonable and unrealistic administrative burden as well as an unreasonable and unrealistic financial burden.[21] [redacted]. If all individual complaints were to be investigated immediately, as advocated by the AP, it would need considerably more manpower than at present. According to [redacted], such unreasonable organisational measures, with their disproportionate costs of implementation, run counter to the concept of a duty to protect personal data as defined in Article 32 of the GDPR.

The AP states first and foremost that the GDPR stipulates the obligations that [redacted] has to meet as a controller. Article 32 of the GDPR requires a data controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk: the ability to detect, address

[20] Paragraph 5 of the views expressed by [redacted].
[21] [redacted].

and report a breach in a timely manner 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 should be reported and every complaint received by [redacted] should be investigated by the Security Team. As soon as a controller becomes aware of a security incident or has been informed of a possible breach by another source, the controller must investigate whether the breach is subject to notification.[23] It is apparent that [redacted] has organised its Data Incident Response Policy in such a way that suspicions and reports of alleged security incidents must be immediately forwarded to the Security Team for assessment. In the opinion of the AP, the fact that this did not occur in this case is at the expense and risk of [redacted]. In this context, the AP once again draws attention to the fact that, on the basis of the various reports from the accommodations, there is virtually no other conclusion that can be reached than that this was a substantial breach that was subject to notification.

Manifest clerical error in the report

[redacted] has argued that paragraph 26 of the investigation report erroneously mentions 2 February 2019 as the date on which [redacted]'s Security Team recorded its findings, but that this date is not mentioned anywhere else in the documents. The AP has assumed that this is a manifest clerical error, since the documents do not provide any basis for the fact that the Security Team presented its findings on 2 February 2019.

For the sake of completeness

Although this is not under discussion in this case, [redacted] has indicated in its expressed views that it attaches considerable importance to data security and immediate action being taken with regard to data breaches. [redacted] considers that it more than meets, and even exceeds, the expectations set out in Article 34 of the GDPR by informing data subjects about data breaches, even where there is unlikely to be a significant risk to the rights and freedoms of data subjects. The AP welcomes such actions but stresses that this does not release [redacted] from the other obligations laid down in the GDPR, such as the notification obligation in Article 33(1) of the GDPR.

3.4.5 Conclusion

In view of the above, the AP is of the opinion that [redacted] infringed Article 33(1) of the GDPR from 16 January 2019 to 6 February 2019, since [redacted] failed to report the personal data breach to the AP in a timely manner and without undue delay.

[22] See Guidelines, p. 14/15.
[23] See the WP29 Guidelines for more details.

Date
10 December 2020

Our reference
[redacted]

4. Fine

4.1 Introduction

As a result of the breach identified above, the AP makes use of its power to impose a fine on [redacted] under Article 58(2)(i) and Article 83(4) of the GDPR, read in conjunction with Article 14(3) of the General Data Protection Regulation (Implementation) Act (*Uitvoeringswet Algemene verordening gegevensbescherming*). The AP applies the 2019 Fining Policy Rules for this purpose (hereinafter: Fining Policy Rules).[24]

In the following, the AP will first briefly set out the system of fines, followed by the reasons for the amount of the fine in the present case.

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

Pursuant to Article 58(2), preamble and under (i) and Article 83(4) of the GDPR, read in conjunction with Article 14(3) of the General Data Protection Regulation (Implementation) Act (*Uitvoeringswet Algemene verordening gegevensbescherming*), the AP is authorised to impose an administrative fine on [redacted] up to € 10,000,000 or up to 2% of the total worldwide annual sales volume in the preceding business year, whichever figure is higher, in the event of an infringement of Article 33(1) of the GDPR.

The AP has adopted Fining Policy Rules for the interpretation of the aforementioned power to impose an administrative fine, including the determination of the amount thereof.[25]

Pursuant to Article 2(2.1) of the 2019 Fining Policy Rules, the provisions in respect of which the AP may impose an administrative fine of up to € 10,000,000 or, in the case of a company, up to 2% of its total worldwide annual sales volume in the preceding business year, whichever figure is the higher, are classified in Appendix 1 into categories I, II or III.

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

Pursuant to Article 2(2.3) of the Fining Policy Rules, the AP sets the basic fine for category III offences 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 adjusting the amount of the basic fine either upwards (up to the maximum in the fine range associated with a breach category) or downwards (to the minimum in that range). The basic fine will be increased or decreased depending on the extent to which the factors referred to in Article 7 give cause to do so.

[24] Government Gazette 2019, 14586, 14 March 2019.
[25] Government Gazette 2019, 14586, 14 March 2019.

Pursuant to Article 7, without prejudice to Articles 3:4 and 5:46 of the General Administrative Law Act (*Algemene wet bestuursrecht*), the AP takes into account the factors derived from Article 83(2) of the GDPR in the Policy Rules referred to under (a) to (k):
a. the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
b. the intentional or negligent character of the infringement;
c. any action taken by the controller [...] to mitigate the damage suffered by data subjects;
d. the degree of responsibility of the controller [...] taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
e. any relevant previous infringements by the controller [...];
f. the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
g. the categories of personal data affected by the infringement;
h. the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller [...] notified the infringement;
i. where measures referred to in Article 58(2) have previously been ordered against the controller [...] concerned with regard to the same subject-matter, compliance with those measures;
j. adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
k. any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Pursuant to Article 9 of the 2019 Fining Policy Rules, the AP is obliged to take the financial circumstances of the offender into account when setting the fine where appropriate. In the event of reduced or insufficient capacity of the offender, the AP may further moderate the fine to be imposed if, after application of Article 8.1 of the Fining Policy Rules, setting a fine within the fine range of the next lower category would, in its opinion, nevertheless result in a disproportionately high fine.

4.3 Amount of the fine

4.3.1. Nature, gravity and duration of the breach

Pursuant to Article 7, preamble and under a, of the Fining Policy Rules, the AP shall take the nature, gravity and duration of the breach into account. In assessing this, the AP shall take into account the nature, scope or purpose of the processing as well as the number of data subjects affected and the extent of the damage suffered by them.

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 (*Handvest van de grondrechten van de Europese Unie*) and Article 16(1) of the Treaty on the Functioning of the European Union (*Verdrag betreffende de werking van de Europese Unie*), everyone has the right to the protection of their personal data. The principles and rules relating to the protection of natural persons with regard to the processing of

their personal data must comply with their fundamental rights and freedoms, in particular their right to the protection of personal data. The purpose of the GDPR is to contribute to the creation of an area of freedom, security and justice and 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 be designed to serve mankind. The right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and weighed against other fundamental rights in accordance with the principle of proportionality. Any processing of personal data must be proper and lawful. 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, including to prevent unauthorised access to or use of personal data and the equipment used for processing.

Notification of breaches should be seen as a means of improving compliance with the rules on the protection of personal data. If a personal data breach takes place or has taken place, it may result in bodily, material or immaterial harm to natural persons or any other economic or social harm to the person concerned. Therefore, as soon as the controller becomes aware of a personal data breach, it should notify the supervisory authority of the personal data breach without undue delay and, if possible, within 72 hours. This will enable the supervisory authority to carry out its tasks and powers properly, as laid down in the GDPR.

[redacted] not only failed to notify the personal data breach without delay, it also failed to do so on several occasions, i.e. on 9, 13 and 20 January 2019, when immediate action should have been expected and which resulted in a (very) undue delay in notifying the AP. Furthermore, instead of making a notification in phases, it has been shown that [redacted] deliberately chose to conduct an in-depth investigation before making the required notification to the supervisory authority. This is not in line with the rules laid down in the GDPR.

The investigation carried out by [redacted]'s Security Team revealed that 4,109 people may have been affected. These were hotel guests, who had booked hotel accommodation at 40 different accommodations through the [redacted] platform. By committing social engineering fraud, unauthorised third parties acquired credit card details as well as name and address details and details of hotel reservations. These are sensitive data which, in the hands of unauthorised persons, can lead to financial loss or other harm.

In view of the nature of the personal data, the amount of the personal data, the number of data subjects affected, the duration of the infringement and the importance of notifying the supervisory authority in a timely manner within 72 hours, the AP considers that this is a serious infringement but sees no reason to increase or decrease the basic amount of the fine.

4.3.2 Intentional or negligent character of the infringement(culpability)

Pursuant to Article 5:46(2) of the General Administrative Law Act (*Algemene wet bestuursrecht*), when imposing an administrative fine, the AP should take into account the extent to which the offender is

culpable. Pursuant to Article 7(b) of the 2019 Fining Policy Rules, the AP should take into account the intentional or negligent character of the infringement.

Article 33(1) of the GDPR stipulates that a personal data breach must be notified without undue delay and, where feasible, not later than 72 hours after the controller has become aware of it. The obligation to notify has been in effect in the Netherlands since 1 January 2016, when this standard was introduced in the Personal Data Protection Act (*Wet bescherming persoonsgegevens*).[26]
Given that a party to which a certain standard applies, such as [redacted] in this case, is deemed to have knowledge of the applicable laws and regulations, the AP takes the view that market parties have their own responsibility to comply with the law. [27]
The AP has also provided market parties with ample information about the applicable laws and regulations, so that it can be assumed that [redacted] was familiar with them. In addition, the notification obligation with regard to data breaches has been widely reported in the media.

In the opinion of AP it should have been sufficiently clear to [redacted] from the legal framework set out above in conjunction with the applicable WP29 Guidelines, which [redacted] could have taken note of prior to the breach, that it should have notified the AP of the breach in a timely manner and without undue delay, but in any event no later than 72 hours after 13 January 2019. In addition, the notification to the AP could have been made on a conditional basis and the notification could have been supplemented afterwards. This option is expressly provided for in the GDPR.
If [redacted] had any doubts about the scope of the notification obligation, a professional and multinational market operator such as [redacted] can be expected to properly obtain information about the restrictions to which its conduct is subject, also according to established case law, in order to adjust its conduct to the scope of that obligation from the outset.[28]

In the opinion of the AP, as an independent party having rights and obligations, [redacted] cannot exculpate itself from the fact that a [redacted] acted contrary to [redacted]'s own protocol, which stipulates that any suspicion of an incident must be immediately forwarded to the Security Team for assessment. This is attributable to [redacted].

[redacted] reported the breach 22 days too late. The AP considers this to be culpable. However, the AP sees no reason to increase or decrease the basic amount of the fine under Article 7(b) of the 2019 Fining Policy Rules.

4.3.3 Actions taken to mitigate the damage suffered

Pursuant to Article 7(c) of the 2019 Fining Policy Rules, the AP is required to take into account any action taken by the controller to mitigate the damage suffered by the data subjects.

[26] Article 34a(1) of the Personal Data Protection Act (*Wet bescherming persoonsgegevens*).
[27] Cf. Trade and Industry Appeals Tribunal 25 June 2013, ECLI:NL:CBB:2013:4, grounds 2.3, Trade and Industry Appeals Tribunal 25 January 2017, ECLI:NL:CBB:2017:14, grounds 5.2, Trade and Industry Appeals Tribunal 8 March 2017, ECLI:NL:CBB:2017:91, grounds 6.
[28] Cf. Trade and Industry Appeals Tribunal 22 February 2012, ECLI:NL:CBB:2012:BV6713, grounds 4.3, Trade and Industry Appeals Tribunal 19 September 2016, ECLI:NL:CBB:2016:290, grounds 8.6., Trade and Industry Appeals Tribunal 19 September 2016, ECLI:NL:CBB:2016:372, grounds 6.3.

In the views expressed by [redacted], it has put forward several specific remedial actions in order to limit possible damage to the data subjects. For example, [redacted] has informed and advised the data subjects about taking measures to reduce the damage. [redacted] has also declared itself willing to compensate any damages (suffered or to be suffered) by the data subjects. Finally, [redacted] immediately informed the affected accommodations and placed warnings on the [redacted] platform.

The AP is of the opinion that, although [redacted] failed to report the breach to the supervisory authority in a timely manner, it is to [redacted]'s credit that it has taken the above measures and declared itself willing to compensate any damages. The fact that [redacted] ultimately acted expeditiously in this respect, which most likely limited the detrimental impact on the data subjects, is taken into account by the AP in determining the level of the fine.

In view of the actions taken by [redacted] to mitigate the damage of the data subjects resulting from the breach, the AP sees reason to reduce the basic amount of the fine by € 50,000 in accordance with Article 7(c) of the 2019 Fining Policy Rules.

4.3.4 Other circumstances

Furthermore, the AP does not see any reason to increase or decrease the basic amount of the fine on the basis of other circumstances, as referred to in Article 7 of the 2019 Fining Policy Rules, insofar as applicable in the present case.

In view of the factors mentioned in Article 7 of the GDPR, the AP sets the amount of the fine for the infringement of Article 33(1) of the GDPR at € 475,000.

4.3.5 Viewpoint of [redacted] and response of the AP

With regard to the imposition of an administrative fine, in the views expressed by [redacted] it primarily argued that the imposition of an administrative fine would not be proportionate. In this respect, [redacted] referred to fines imposed by the Lithuanian, Hungarian and Hamburg authorities for infringements of Article 33(1) of the GDPR.[29] [redacted] takes the viewpoint that, within the framework of the idea of harmonisation, the same fines should be imposed for similar offences within Europe.

At present, no common principles for the calculation of fines have been agreed at European level. Consequently, the AP independently applies its own Fining Policy Rules for the calculation of fines. In addition, the AP is assessing this case on its own merits and thus according to the specific facts and circumstances of the case. It goes without saying that these are different in each case and therefore not comparable with each other. Finally, the fine decisions of other privacy supervisory authorities as expounded by [redacted] in its views, were not reached on the basis of the consistency mechanism, as laid down in Article 60 of the GDPR, and the AP is therefore not bound by those decisions and is not bound to impose a fine of an equal amount in the present case.

[29] Paragraph 9.2(a) of the views expressed by [redacted].

[redacted] also argued that, in the absence of clear guidelines from the AP and the European Data Protection Board (*Europees Comité voor Gegevensbescherming*) in respect of the reasons for a delay in reporting a data breach, the imposition of an administrative fine would violate the *lex certa* principle.

The AP also does not agree with this viewpoint of [redacted] and refers to what has been considered in paragraphs 3.4.4 and 4.3.2 of this decision.

Finally, [redacted] argued as a second alternative that if the AP nevertheless decides to impose a fine, it should be reduced to the lowest fine in category II in accordance with Article 6 in conjunction with Article 8.1 of the Fine Policy Rules.

With regard to the nature, gravity and duration of the infringement, [redacted] has briefly argued that the preventive and corrective measures taken by [redacted] have limited both the number of people affected and the extent of the damage.

However, with reference to paragraph 4.3.1, the AP sees no reason to refrain from imposing an administrative fine or to reduce the amount of the fine.

With regard to the intentional or negligent character of the infringement, [redacted] has argued that the breach is not the result of any intention or negligence on the part of [redacted] and refers to the technical and organisational measures taken to prevent social engineering incidents and to limit the consequences.

The AP rejects this viewpoint. As stated in paragraph 4.3.2, the AP is of the opinion that negligence is attributable to [redacted]. The AP sees no reason to increase or decrease the basic amount of the fine.

With regard to the measures taken to limit the damage, [redacted] argues that the technical and organisational measures it has taken are appropriate and may even exceed the requirements of the GDPR.

As discussed in paragraph 4.3.3 above, the AP considers this as a reason to reduce the basic amount of the fine.

With regard to the degree of responsibility given the technical and organisational measures taken by [redacted], in accordance with Articles 25 and 32 of the GDPR, [redacted] has argued that its systems and organisation are designed in such a way that the principles of data protection can be effectively implemented, reiterating that, given the measures taken and the nature of the incident, [redacted] cannot be held liable for the data breach and the alleged infringement.

The AP does not share this viewpoint. A professional party such as [redacted] may be expected to be fully aware of and comply with the standards applicable to it, also given the nature and extent of the processing. As previously considered in paragraph 4.3.2 of this decision, [redacted] is fully responsible for the infringement. Consequently, the AP does not see any reason to reduce the fine in this case either.

With regard to previous relevant breaches of the GDPR, [redacted] has argued that it had not previously received a notice from the AP regarding alleged breaches of Article 33(1) of the GDPR.

The AP fails to understand why this viewpoint of [redacted] should lead to a reduction in the basic amount of the fine. The fact that the AP has not previously sent a notice to [redacted] regarding an identical offence does not lead to a reduction in the amount of the fine.
[redacted].

With regard to the cooperation between [redacted] and the AP to remedy the alleged infringement and mitigate its possible adverse effects, [redacted] has argued that it fully cooperated with the AP by answering all questions in a timely manner and that if the AP had asked for an explanation for the delay in the notification then this explanation would have been given.

The AP sees no reason to reduce the amount of the fine in this regard. The AP considers that [redacted]'s cooperation has not gone beyond its legal obligation to comply with Article 33(1) of the GDPR. [redacted] did not cooperate with the AP in any special way.

With regard to the other factors, [redacted] has briefly argued that the personal data does not fall under special categories of personal data or belong to a vulnerable group of persons, that [redacted] has been fully transparent to the data subjects and that it notified the AP of the data breach itself. Finally, [redacted] has argued that if it had notified the AP earlier, this would not have led to any other action on [redacted]'s part or to further reduction of the risks to the privacy of the data subjects. According to [redacted], none of the data subjects suffered any damage at all as a result of the timing of the notification.

Again, the AP does not agree with the views expressed by [redacted]. Despite the fact that, as far as we know, the breach did not affect any special personal data, that [redacted] independently informed those concerned and that the (financial) consequences were limited for the data subjects, the AP sees no reason to further reduce the amount of the fine because of the seriousness of the infringement and [redacted]'s culpability. The AP refers to paragraphs 4.3.1 and 4.3.2 for its reasoning.

4.3.6 Proportionality and maximum legal fine

Finally, on the basis of the principle of proportionality laid down in Articles 3:4 and 5:46 of the General Administrative Law Act (*Algemene wet bestuursrecht*), the AP assesses whether the application of its policy for determining the level of the fine would lead to a disproportionate outcome in view of the circumstances of the specific case. The application of the principle of proportionality, according to the 2019 Fining Policy Rules, means that the AP must take into account the financial circumstances of the offender where appropriate when setting the fine.

Date
10 December 2020

Our reference
[redacted]

In light of all the above considerations, the AP considers that the level of the fine to be imposed does not lead to a disproportionate outcome. In addition, this decision has been taken by means of the consistency mechanism provided for in the GDPR. The other European supervisory authorities involved have endorsed the assessment of the AP.

Given its financial position, the AP sees no reason to assume that [redacted] would not be able to bear a fine of € 475,000.

4.4 Conclusion

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

5. Operative part

Fine

AP imposes an administrative fine of **€ 475,000** (in words: four hundred and seventy-five thousand euros) on [redacted] for the infringement of Article 33(1) of the GDPR.[30]

Yours sincerely,
Dutch Data Protection Authority

[redacted]

Remedy clause
If you do not agree with this decision, you can submit a notice of objection, either electronically or on paper, to the Dutch Data Protection Authority within six weeks of the date on which the decision was sent digitally or on paper.
The submission of an objection suspends the operation of the decision imposing the administrative fine, pursuant to Article 38 of the General Data Protection Regulation (Implementation) Act (*Uitvoeringswet Algemene verordening gegevensbescherming*).
To submit an objection digitally, see www.autoriteitpersoonsgegevens.nl, under the heading Objection to a decision, which is at the bottom of the page under the heading Contact with the Personal Data Authority.

[30] The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (*Centraal Justitieel Incassobureau*).

Date
10 December 2020

Our reference
[redacted]

The address for the submission of an objection on paper is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.
Please include 'Administrative objection' on the envelope and 'Objection' in the subject line of your letter.
At a minimum your notice of objection should include:
- your name and address;
- the date of your objection;
- the reference mentioned in this letter (case number) or a copy of this decision should be attached;
- the reasons why you disagree with this decision;
- your signature.