AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Aangetekend
Booking.com B.V.
De Raad van Bestuur
t.a.v. [VERTROUWELIJK]
Postbus 1639
1000 BP Amsterdam

Datum
10 december 2020

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Besluit tot het opleggen van een bestuurlijke boete

Geachte [VERTROUWELIJK],

De Autoriteit Persoonsgegevens (AP) heeft besloten aan Booking.com B.V. (Booking) een **bestuurlijke boete** van **€ 475.000,--** op te leggen. De AP is van oordeel dat Booking artikel 33, eerste lid, van de Algemene Verordening Gegevensbescherming (AVG) vanaf 16 januari 2019 tot en met 6 februari 2019 heeft overtreden, omdat Booking heeft nagelaten een inbreuk in verband met persoonsgegevens binnen 72 uur nadat daarvan kennis was genomen, te melden bij de AP.

Hierna wordt het besluit nader toegelicht. Hoofdstuk 1 bevat een inleiding en hoofdstuk 2 beschrijft het wettelijk kader. In hoofdstuk 3 beoordeelt de AP haar bevoegdheid, de verwerkingsverantwoordelijkheid en de overtreding. In hoofdstuk 4 wordt de (hoogte van de) bestuurlijke boete uitgewerkt en hoofdstuk 5 bevat het dictum en de rechtsmiddelenclausule.

Bijlage(n) 1

1. Inleiding

1.1 Betrokken rechtspersonen

Booking is een besloten vennootschap die statutair is gevestigd op de Herengracht 597 (1017 CE) te Amsterdam. Booking is op 23 juni 1997 opgericht en is in het register van de Kamer van Koophandel ingeschreven onder nummer 31047344. Booking biedt een online platform aan waarop Trip Providers, zoals accommodaties, hun producten en diensten ter reservering kunnen aanbieden en gebruikers van het platform deze vervolgens kunnen reserveren.
Booking is, via diverse Nederlandse en Engelse rechtspersonen, een indirect 100% dochter van het aan de Amerikaanse NASDAQ Stock Market genoteerde Booking Holdings Inc. Laatstgenoemde had blijkens haar openbare en geconsolideerde jaarrekening over 2019 een omzet van 15,1 miljard dollar (EUR 13.727.410.000) en een netto resultaat van 4,9 miljard dollar (EUR 4.454.590.000).

1.2 Aanleiding onderzoek

Op 7 februari 2019 heeft Booking bij de AP een melding van een inbreuk in verband met persoonsgegevens (datalek) gedaan. Een onbekende derde had toegang verkregen tot een reserveringssysteem van Booking door zich bij meerdere accommodaties voor te doen als medewerker van Booking. Hierbij zijn de persoonsgegevens van meerdere betrokkenen, die via het platform van Booking hotelreserveringen hadden gedaan, gecompromitteerd. Omdat Booking in het meldingsformulier heeft aangegeven dat Booking de inbreuk in verband met persoonsgegevens op 10 januari 2019 had ontdekt, is de AP een onderzoek gestart naar de naleving van artikel 33, eerste lid, van de AVG door Booking.

1.3 Procesverloop

Bij brief van 12 februari 2019 heeft de AP aan Booking een inlichtingenverzoek toegestuurd. Dit verzoek is op 26 februari 2019 tevens per e-mail toegezonden.

Op 27 februari 2019 heeft Booking de melding van bovengenoemde inbreuk in verband met persoonsgegevens inhoudelijk aangevuld.

Bij brief van 1 maart 2019 heeft Booking schriftelijk gereageerd op het inlichtingenverzoek van 12 februari 2019.

Bij brief van 6 maart 2019 heeft de AP aan Booking een aanvullend inlichtingenverzoek toegestuurd.

Bij brief van 13 maart 2010 heeft Booking schriftelijk gereageerd op het verzoek van 6 maart 2019.

Bij e-mail van 19 maart 2019 heeft de AP aan Booking een aanvullend verzoek om informatie toegezonden.

Bij e-mail van 19 maart 2019 heeft Booking de gevraagde informatie en een aanvullend document aan de AP toegezonden.

Vanwege het grensoverschrijdende karakter van de zaak heeft de AP de overige toezichthoudende autoriteiten op 19 maart 2019 op de hoogte gebracht van onderhavige zaak, waarbij tevens is vastgesteld dat de AP optreedt als leidende toezichthouder nu het hoofdkantoor van Booking gevestigd is in Nederland.

Bij brief van 16 juli 2019 heeft de AP een voornemen tot handhaving en het onderzoeksrapport aan Booking toegezonden en Booking daarbij in de gelegenheid gesteld om haar zienswijze kenbaar te maken. Booking heeft bij brief van 3 september 2019 schriftelijk haar zienswijze gegeven over dit voornemen en het daaraan ten grondslag gelegde rapport.

Op 23 oktober 2020 heeft de AP conform artikel 60 van de AVG een ontwerpbesluit aan de betrokken toezichthoudende autoriteiten voorgelegd. Hiertegen zijn geen bezwaren ingediend.

2.Wettelijk kader

2.1 Reikwijdte AVG

Ingevolge artikel 2, eerste lid, van de AVG is deze verordening van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Ingevolge artikel 3, eerste lid, van de AVG is deze verordening van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt.

Ingevolge artikel 4 van de AVG wordt voor de toepassing van deze verordening verstaan onder:
1. “Persoonsgegevens”: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”); […].
2. “Verwerking”: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés […].
7. “Verwerkingsverantwoordelijke”: een […] rechtspersoon […] die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; […].
12. “Inbreuk in verband met persoonsgegevens”: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

23. “Grensoverschrijdende verwerking”: […] b) verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke […], waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden.

2.2 Melding inbreuk in verband met persoonsgegevens

Ingevolge artikel 4, twaalfde lid, van de AVG wordt onder een “inbreuk in verband met persoonsgegevens” verstaan: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Ingevolge artikel 33, eerste lid, van de AVG dient een verwerkingsverantwoordelijke een inbreuk in verband met persoonsgegevens zonder onredelijke vertraging te melden en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (…). In het geval de melding aan de toezichthouder niet binnen 72 uren plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

2.3 Competentie leidende toezichthoudende autoriteit

Ingevolge artikel 55, eerste lid, van de AVG heeft elke toezichthoudende autoriteit de competentie op het grondgebied van haar lidstaat de taken uit te voeren die haar overeenkomstig deze verordening zijn opgedragen en de bevoegdheden uit te oefenen die haar overeenkomstig deze verordening zijn toegekend.

Ingevolge artikel 56, eerste lid, van de AVG is de toezichthoudende autoriteit van de hoofdvestiging of de enige vestiging van de verwerkingsverantwoordelijke (…) onverminderd artikel 55 competent op te treden als leidende toezichthoudende autoriteit voor de grensoverschrijdende verwerking door die verwerkingsverantwoordelijke (…) overeenkomstig de procedure van artikel 60.

3.Beoordeling

3.1 Competentie AP

In het onderhavige geval gaat het om een verwerking van persoonsgegevens door Booking waardoor betrokkenen in meer dan één lidstaat wezenlijke gevolgen hebben ondervonden.[1] Hierdoor is er sprake van een grensoverschrijdende verwerking in de zin van artikel 4, onderdeel 23 sub b, van de AVG. De AP stelt vast dat zij op grond van artikel 56 van de AVG competent is op te treden als leidende toezichthoudende autoriteit nu de hoofdvestiging van Booking is gevestigd in Amsterdam.

[1] Zie hiervoor paragraaf 3.4.2.

3.2 Verwerking van persoonsgegevens

Volgens artikel 4, onder 1, van de AVG betreffen persoonsgegevens alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, door bijvoorbeeld een of meer elementen die kenmerkend zijn voor de fysieke of fysiologische identiteit van die natuurlijke persoon.

Artikel 4, onder 2, van de AVG, definieert het begrip verwerking als een bewerking van persoonsgegevens, zoals het verzamelen, vastleggen, opslaan, opvragen, raadplegen of gebruiken daarvan.

Booking biedt een online reserveringsplatform aan waar zogenoemde "Trip Providers", zoals accommodatieverstrekkers en andere aanbieders, beschikbare accommodaties, vluchten, huurauto's en dagtrips aanbieden. Via het platform kunnen bezoekers onder meer naar overnachtingsadressen en dagtrips zoeken waarna deze via het platform kunnen worden gereserveerd.
Bij een reservering via het platform van Booking worden door de betrokkene persoonsgegevens zoals contact-, reserverings- en betalingsgegevens ingevoerd. Booking verstrekt vervolgens de details van de reservering aan de Trip Provider via het Extranet van Booking.[2] Het Extranet van Booking is een online administratief dashboard met beveiligde toegang. Naast toegang tot reserveringsgegevens in het Extranet, hebben de Trip Providers toegang tot alle informatie die op de Trip Provider pagina bij Booking.com wordt weergegeven, inclusief de betalingsmogelijkheden en beleidsregels.
Om toegang te verkrijgen tot het Extranet dient de Trip Provider een username, password en 'two factor authentication pin code' in te geven. Nadat de Trip Provider is ingelogd op het Extranet kunnen zij de noodzakelijke reserveringsgegevens van de gasten raadplegen.

Het naar aanleiding van de inbreuk ingeschakelde Security Team van Booking heeft vastgesteld dat een onbekende derde partij toegang heeft verkregen tot het Extranet van Booking. De bevindingen van het Security Team zijn vastgelegd in een zogenoemd Security Incident Summary rapport. Uit het in het dossier opgenomen Security Incident Summary rapport van 28 februari 2019 blijkt dat onder meer de volgende gegevens van gasten zijn gecompromitteerd die in het Extranet werden bewaard: voornaam, achternaam, adres, telefoonnummer, check-in en check-uit datum, totaalprijs, reserveringsnummer, prijs per nacht, eventuele correspondentie tussen accommodatie en gast en ten aanzien van 283 betrokkenen de creditcard gegevens waarvan 97 met de 'card verification code'.[3]

De gemelde inbreuk in verband met persoonsgegevens van Booking ziet aldus onder meer op namen, adresgegevens, telefoonnummers en creditcardgegevens van hotelgasten. Nu dit informatie betreft over geïdentificeerde of identificeerbare natuurlijke personen, zijn voornoemde gegevens aan te merken als persoonsgegevens zoals bepaald in artikel 4, eerste onderdeel, van de AVG.

[2] Dossierstuk 1: melding inbreuk in verband met persoonsgegevens 7-2-2019, p3.
[3] Dossierstuk 9, Antwoorden van Booking op verzoek om inlichtingen, Bijlage 5.

De AP stelt vast dat via het Extranet een bewerking van persoonsgegevens plaatsvindt: de gegevens worden in het Extranet vastgelegd, opgeslagen en verder ontsloten. Het geheel van bewerkingen in het Extranet is een verwerking van persoonsgegevens als bedoeld in artikel 4, onderdeel twee, van de AVG.

3.3 Verwerkingsverantwoordelijke

In het kader van de vraag wie verantwoordelijk kan worden gehouden voor het begaan van een overtreding van de AVG, dient te worden bepaald wie als verwerkingsverantwoordelijke kan worden aangemerkt zoals bedoeld in artikel 4, onder 7, van de AVG. Daarbij is van belang om vast te stellen wie het doel van en de middelen voor de verwerking van persoonsgegevens – in dit geval de verwerking van persoonsgegevens van betrokkenen die gebruik maken van het platform van Booking – vaststelt.

De AP is van oordeel dat Booking het doel en de middelen bepaalt voor de verwerking van de persoonsgegevens die betrekking hebben op reserveringen die via Booking.com worden gedaan en vervolgens via het Extranet van Booking worden verwerkt. De AP licht dit als volgt toe.

In de Privacyverklaring van Booking, zoals geplaatst op diens website, staat vermeld welke persoonsgegevens door Booking worden verwerkt alsmede de redenen waarom en de wijze waarop deze worden verwerkt. De Privacyverklaring vermeldt onder meer dat Booking gegevens deelt met derden, waaronder de "Reisaanbieder", oftewel de Trip Provider. Dat de gegevens met de reisaanbieder worden gedeeld via het Extranet blijkt onder meer uit de melding van de inbreuk op 7 februari 2019 en de zienswijze van Booking.[4] De Privacyverklaring vermeldt tevens expliciet dat het verwerken van de hiervoor genoemde persoonsgegevens wordt gedaan door Booking (Herengracht 597, 1017 CE Amsterdam, Nederland).[5]

Daarnaast bepaalt Booking de invulling van de beveiliging van het Extranet door het treffen van beveiligingsmaatregelen voor de toegangscontrole zoals de "two factor authentication" (waarvan de code tevens door Booking wordt gegenereerd).[6] Verder heeft Booking, naast andere beveiligingsmaatregelen, een datalekmeldprocedure opgezet die ziet op incidenten betreffende het Extranet.[7]

De AP stelt daarom op grond van het voornoemde vast dat Booking het doel en de middelen bepaalt voor de verwerking van de persoonsgegevens die betrekking hebben op reserveringen die via het platform van Booking worden gedaan, en die via het Extranet (een systeem dat door Booking wordt gebruikt en beheerd) worden verwerkt.

Booking heeft in haar zienswijze enerzijds aangevoerd dat Booking de verwerkingsverantwoordelijke is voor de klantgegevens die met betrekking tot haar platform worden verwerkt.[8] Anderzijds stelt Booking

[4] Dossierstuk 20: onderzoeksrapport, randnummer 17 e.v., zienswijze randnummer 2.3 e.v.
[5] Onder het kopje "Wie is verantwoordelijk voor het verwerken van persoonsgegevens via Booking.com en hoe ons te bereiken?".
[6] Zienswijze, randnummer 2.5.
[7] Zienswijze, randnummers 2.6, 3.2 en 3.3.
[8] Zienswijze, randnummer 2.2.

dat de Trip Provider als verwerkingsverantwoordelijke acteert voor de klantgegevens die via het Extranet beschikbaar worden gesteld en dat Booking zich niet verantwoordelijk acht voor gegevensverwerkingsactiviteiten van de Trip Providers.[9]

Dat Trip Providers tevens in het Extranet kunnen (fysiek) en daarin persoonsgegevens kunnen verwerken, laat onverlet dat Booking verwerkingsverantwoordelijke is voor het Extranet. En zodoende dus ook verantwoordelijk voor wat er met de persoonsgegevens in het Extranet gebeurt. Het argument van Booking treft dan ook geen doel.
Dat Booking zichzelf ook als verwerkingsverantwoordelijke ziet voor de persoonsgegevens die via het Extranet worden verwerkt, blijkt mede uit het feit dat Booking de inbreuk in verband met persoonsgegevens op 7 februari 2019 heeft gemeld bij de AP en ook in haar zienswijze stelt Booking verwerkingsverantwoordelijke te zijn voor de klantgegevens die via haar platform worden verwerkt.[10]

Op grond van het voorgaande stelt de AP vast dat Booking de verwerkingsverantwoordelijke is in de zin van artikel 4, onderdeel zeven, van de AVG.

3.4 Overtreding inzake melden inbreuk

3.4.1 Inleiding

Artikel 33, eerste lid, van de AVG bepaalt dat indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de (…) bevoegde toezichthoudende autoriteit meldt, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. In het geval de melding aan de toezichthouder niet binnen 72 uren plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

De AP zal in deze paragraaf eerst de feiten schetsen en daarna beoordelen of Booking de inbreuk in verband met persoonsgegevens (tijdig) bij de toezichthouder had moeten melden.

3.4.2 Feiten

9 januari 2019
Op 9 januari 2019 meldt een accommodatie [11](I) in de Verenigde Arabische Emiraten aan een [VERTROUWELIJK] van Booking per e-mail dat een gast heeft geklaagd over het feit dat deze per e-mail was benaderd door een onbekende partij die zich voordeed als medewerker van de accommodatie met de melding dat diens creditcard niet werkte en of de gast zijn geboortedatum of andere bankkaartgegevens wilde opgeven zodat een gereserveerde overnachting kon worden aanbetaald. De accommodatiemanager vraagt in zijn e-mailbericht aan Booking het incident te onderzoeken nu de accommodatie vanuit het Extranet niet kan beschikken over e-mailadressen van klanten en hij denkt dat waarschijnlijk sprake is van

[9] Zienswijze, randnummer 2.3.
[10] Zienswijze, randnummer 2.2.
[11] Oftewel: een Trip Provider.

een (data)lek bij Booking aangezien de onbekende partij op de hoogte was van de, via het platform van Booking gemaakte, reservering bij de accommodatie.

E-mail van 9 januari 2019 18:00 uur
"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 [VERTROUWELIJK] 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 [VERTROUWELIJK] 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 [VERTROUWELIJK] 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 […]"

Bij voornoemde e-mail was de e-mail gevoegd die de betrokkene van de onbekende derde partij had ontvangen. Uit deze e-mail blijkt dat de onbekende derde partij met behulp van de reserveringsgegevens van de betrokkene persoons- en/of betalingsgegevens tracht te verkrijgen.

E-mail van 8 januari 2019 22:32 uur
"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 januari 2019
Op 13 januari 2019 meldt dezelfde accommodatie (I) bij voornoemde [VERTROUWELIJK] van Booking dat een zelfde soort klacht van een andere gast is ontvangen. Een onbekende partij had zich – ditmaal telefonisch – bij de gast bekend gemaakt namens Booking waarbij getracht werd diens creditcard- en persoonsgegevens te verkrijgen.

E-mail van 13 januari 2019 10:18 uur
"Subject: RE: [External Fraud] / Leaked Guest Information / URGENT
Hi […]

Datum
10 december 2020

Ons kenmerk
[VERTROUWELIJK]

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
[…] [VERTROUWELIJK]"

20 januari 2019
Op 20 januari 2019 meldt accommodatie I dat een derde gast zich heeft beklaagd omdat hij telefonisch was benaderd met het verzoek om zijn creditcardgegevens door te geven. De accommodatiemanager geeft aan de [VERTROUWELIJK] van Booking door dat gezien de ernst van de situatie de kwestie zal worden opgeschaald naar het hoofdkantoor.

E-mail van 20 januari 2019 17:14 uur
"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,
[…] [VERTROUWELIJK]"

Op eveneens 20 januari 2019 meldt een tweede accommodatie zich bij Booking dat sprake is van "an alarming situation with Booking.com reservations". Diverse gasten die via Booking hadden gereserveerd, zijn telefonisch benaderd met het verzoek hun creditcardgegevens door te geven. Ook deze accommodatie vraagt de *[VERTROUWELIJK]* van Booking onderzoek te doen.

E-mail van 20 januari 2019 11:35 uur
"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 [VERTROUWELIJK] password as well as my own password.

Can you please look into this?

Thank you,
[…]
[VERTROUWELIJK]"

Booking hanteert het beleid dat vermoedens en meldingen van incidenten direct dienen te worden doorgezet naar het Security Team van Booking.[12]
De [VERTROUWELIJK] van Booking die door de accommodaties op de hoogte waren gebracht van de frauduleuze handelingen door een onbekende derde partij hebben het Security Team van Booking op 31 januari 2019 ingelicht.
Op 4 februari 2019 heeft het Security Team van Booking haar eerste onderzoek afgerond en geconcludeerd dat het Privacy Team van Booking diende te worden geïnformeerd. De onderzoeksbevindingen van het Security Team zijn vastgelegd in het eerdergenoemde Security Incident Summary Report van 28 februari 2019.[13]

Uit dit onderzoek door het Security Team is gebleken dat 40 accommodaties in de Verenigde Arabische Emiraten het slachtoffer zijn geworden van social engineering fraude, waarbij de persoonsgegevens van mogelijk 4109 betrokkenen zijn gecompromitteerd. Een onbekend gebleven derde partij heeft zich telefonisch voorgedaan als medewerker van Booking om de gebruikersnaam, het wachtwoord en de twee-factor authenticatiecode ("2FA") van de accommodaties te verkrijgen. Met deze informatie kon de derde partij inloggen op het Extranet van Booking waarin reserveringsgegevens van gasten zijn opgenomen. Het Security Team heeft vastgesteld dat 19 december 2018 de startdatum van het veiligheidsincident is geweest. De betrokken personen waren zowel afkomstig uit Europa (onder meer Groot Brittannië, Frankrijk, Ierland, Zwitserland, België, Nederland) als uit andere delen van de wereld (onder meer Zuid Afrika, Amerika, Canada en Bahrein).

De betrokken persoonsgegevens betroffen onder meer voornaam, achternaam, adres, telefoonnummer, check-in en check-uit datum, totaalprijs, reserveringsnummer, prijs per nacht, eventuele correspondentie tussen accommodatie en gast en creditcardgegevens ten aanzien van 283 betrokkenen waarvan 97 met de 'card verification code'.

Op 4 februari 2019 heeft het Security Team het Privacy Team van Booking geïnformeerd over de uitkomsten van het onderzoek. Tevens zijn op 4 februari 2019 alle betrokkenen door Booking op de hoogte gebracht.[14]

Het Privacy Team van Booking heeft op 6 februari 2019 vastgesteld dat sprake was van een datalek dat diende te worden gemeld bij de AP.

[12] Zie dossierstuk 15, Antwoord op verzoek om inlichtingen m.b.t. interne beleidsdocumenten datalekken.
[13] Dossierstuk 9, Antwoorden van Booking op verzoek om inlichtingen, Bijlage 5.
[14] Meldingsformulier en zienswijze, randnummer 4.4 onder d.

Op 7 februari 2019 heeft Booking bij de AP een melding gedaan als bedoeld in artikel 33, eerste lid, van de AVG.[15]

3.4.3 Beoordeling

Artikel 33, eerste lid, van de AVG bepaalt dat indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de (…) bevoegde toezichthoudende autoriteit meldt, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Voordat de melding wordt gedaan, dient door de verwerkingsverantwoordelijke derhalve eerst te worden beoordeeld of sprake is van een inbreuk in verband met persoonsgegevens. Vervolgens dient te worden beoordeeld of de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Een inbreuk in verband met persoonsgegevens

Zoals de AP in paragraaf 3.4.2 heeft vastgesteld heeft een onbekende derde partij toegang gehad tot het Extranet van Booking en op die manier ongeoorloofde toegang gekregen tot de door Booking verwerkte gegevens met betrekking tot reserveringen van gasten bij accommodaties. Booking betwist ook niet dat sprake was van een inbreuk in verband met persoonsgegevens. Daarmee stelt de AP vast dat er sprake is van een inbreuk in verband met persoonsgegevens in de zin van artikel 4, onderdeel 12, van de AVG.

Risico voor de rechten en vrijheden van natuurlijke personen

Na de ongeoorloofde verkrijging van voornoemde persoonsgegevens heeft de onbekende derde partij vervolgens geprobeerd om met behulp van deze persoonsgegevens creditcard gegevens te verkrijgen van gasten die hadden geboekt via het online platform van Booking. Daarmee stelt de AP niet alleen vast dat het waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen maar ook dat dit risico zich heeft gematerialiseerd nu de onbekende derde partij contact heeft opgenomen met vele, zo niet honderden, betrokkenen om te proberen hen op basis van oneigenlijke gronden creditcard gegevens afhandig te maken. Door de inbreuk op de vertrouwelijkheid van de gegevens bestond niet alleen een risico op financiële schade maar ook op identiteitsfraude of enig ander nadeel. De AP stelt daarom vast dat de inbreuk in verband met persoonsgegevens een risico inhield voor de rechten en vrijheden van natuurlijke personen.

Melding aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit

In paragraaf 3.3 is vastgesteld dat Booking verwerkingsverantwoordelijke is. In paragraaf 3.1 heeft de AP vastgesteld dat zij op grond van artikel 56 van de AVG competent is op te treden als leidende toezichthoudende autoriteit nu de hoofdvestiging van Booking is gevestigd in Amsterdam. Booking heeft de inbreuk op 7 januari 2019 gemeld bij de AP. Daarmee heeft Booking de melding gedaan bij de in onderhavige zaak bevoegde autoriteit overeenkomstig artikel 55 van de AVG.

[15] Dossierstuk 1, Melding inbreuk in verband met persoonsgegevens 7-2-2019. P 5.

Melding uiterlijk 72 uur nadat de verwerkingsverantwoordelijk kennis van heeft genomen van een inbreuk in verband met persoonsgegevens
De Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679[16] (hierna: Richtsnoeren), opgesteld door de Groep Gegevensbescherming artikel 29 (hierna: WP29), bevatten een toelichting op de meldplicht(en) in de AVG en bieden een handvat hoe bij diverse soorten inbreuken dient te worden gehandeld.

Wanneer een verwerkingsverantwoordelijke precies kan worden geacht kennis te hebben gekregen van een bepaalde inbreuk hangt af van de omstandigheden van de specifieke inbreuk. Volgens de WP29 moet een verwerkingsverantwoordelijke worden geacht kennis te hebben gekregen van een inbreuk in verband met persoonsgegevens wanneer hij een redelijke mate van zekerheid heeft dat zich een veiligheidsincident heeft voorgedaan dat tot de compromittering van persoonsgegevens heeft geleid.

De AP is van oordeel dat Booking in elk geval op 13 januari 2019 kennis had van de inbreuk in verband met persoonsgegevens en overweegt hiertoe het volgende.

Op 9 januari 2019 ontving de [VERTROUWELIJK] van Booking een eerste signaal, via een e-mail afkomstig van een Trip Provider in de Verenigde Arabische Emiraten (accommodatie I) dat er bij de betrokkene én de Trip Provider een serieus vermoeden bestond dat sprake was van een datalek. De betrokkene was op 8 januari 2019 via e-mail benaderd door een (onbekend gebleven) derde die bekend was met de via het platform van Booking gemaakte reservering én aan de hand van die reserveringsgegevens meer persoonsgegevens trachtte te verkrijgen waarmee zogenaamd een betaling van een overnachting in orde zou kunnen worden gemaakt. Uit de bewuste e-mail van 8 januari 2019, welke is opgenomen in het dossier, blijkt dat deze tevens een pdf-bestand bevatte met de reserveringsdetails. Dit pdf-bestand is door Booking overigens niet overgelegd en derhalve niet opgenomen in het dossier.

Naar het oordeel van de AP had voornoemd incident door (de [VERTROUWELIJK] van) Booking moeten worden doorgezet aan het Security Team van Booking voor het doen van verder onderzoek nu de e-mail in kwestie de exacte reserveringsdetails van de betrokkene bevatte en tevens vaststond dat de boeking via het platform van Booking was gemaakt. Dit te meer nu de Trip Provider reeds tot de conclusie was gekomen dat sprake moest zijn van een beveiligingsincident en op grond van de hem ter beschikking staande gegevens reeds een eerste afweging had gemaakt. Dit blijkt tevens uit het door de accommodatiemanager benoemde onderwerp van de e-mail: "[External] Fraud / Leaked Guest Information/ URGENT". Het Security Team had reeds toen een verkennend onderzoek kunnen beginnen.
Op 13 januari 2019 heeft (dezelfde [VERTROUWELIJK] van) Booking een tweede signaal ontvangen van voornoemde Trip Provider. De betrokkene in kwestie was telefonisch naar zijn persoonsgegevens gevraagd door iemand die zich voordeed als medewerker van Booking en die op de hoogte was van de door de betrokkene via het platform van Booking gemaakte reservering. De accommodatiemanager heeft in zijn e-mail aan de [VERTROUWELIJK] van Booking nadrukkelijk aangegeven het incident gelijkwaardig te achten

[16] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, Groep Gegevensbescherming Artikel 29, laatstelijk herzien en goedgekeurd op 6 februari 2018, 18/NL WP250rev.01.

aan het eerdere incident en meende wederom dat sprake moest zijn van een datalek aan de kant van Booking.

De AP is van oordeel dat Booking in ieder geval op 13 januari 2019 geacht wordt kennis te hebben van de inbreuk in verband met persoonsgegevens, omdat Booking met bovenstaande informatie een redelijke mate van zekerheid had dat zich een veiligheidsincident heeft voorgedaan dat tot de compromittering van door Booking verwerkte persoonsgegevens heeft geleid. De accommodatiemanager van de Trip Provider had immers reeds geconcludeerd dat sprake moest zijn van een beveiligingsincident met betrekking tot het Extranet, waarbij persoonsgegevens van gasten waren gecompromitteerd.

Gezien de alarmerende situatie had Booking het incident direct moeten doorzetten aan het Security Team van Booking zodat onderzoek naar de omvang van de inbreuk kon worden gedaan, hetgeen echter door Booking tot 31 januari 2019 is nagelaten.

Op grond van het voorgaande heeft de in artikel 33, eerste lid, van de AVG voorgeschreven termijn van 72 uur voor het melden van een inbreuk bij de AP een aanvang genomen op 13 januari 2019. Dientengevolge had Booking de inbreuk in verband met persoonsgegevens uiterlijk op 16 januari 2019 bij de AP moeten melden. Vaststaat dat Booking deze melding pas op 7 februari 2019 heeft gedaan, derhalve 22 dagen te laat.

Dit geldt tevens indien zou worden uitgegaan van de datum 20 januari 2019, de datum waarop naast accommodatie I zich tevens een andere Trip Provider (accommodatie II) in de Verenigde Arabische Emiraten bij de [VERTROUWELIJK] van Booking met soortgelijke incidenten heeft gemeld. Ook in deze berichtgeving per e-mail is het onderwerp opzichtig met hoofdletters aangegeven: **SECURITY BREACH**. De inbreuk in verband met persoonsgegevens zou in dat geval 15 dagen te laat bij de toezichthoudende autoriteit zijn gemeld.

3.4.4 Zienswijze Booking en reactie AP

Melding inbreuk
Booking heeft in haar zienswijze primair het standpunt ingenomen dat er geen sprake is van een overtreding nu zij pas op 4 februari 2019, na afronding van het interne onderzoek, kennis heeft genomen van de inbreuk waarna deze tijdig en zonder onredelijke vertraging binnen 72 uur na kennisname is gemeld, hetgeen volgens Booking in lijn is met artikel 33, eerste lid, van de AVG.

De AP volgt dit standpunt niet. Zoals blijkt uit het voorgaande heeft de AP vastgesteld dat Booking op 13 januari 2019 kennis heeft gekregen van de inbreuk. Hieruit volgt dat Booking de inbreuk in verband met persoonsgegevens niet conform het bepaalde in artikel 33, eerste lid, van de AVG heeft gemeld.

Meldingen accommodaties
Ten aanzien van het signaal van accommodatie I op 9 januari 2019 heeft Booking in haar zienswijze aangevoerd dat de [VERTROUWELIJK] van Booking destijds de afweging had gemaakt dat er geen aanleiding bestond om de melding op te schalen naar het Security Team van Booking, omdat de

betrokkene in kwestie was benaderd per e-mail. Booking stelt dat e-mailadressen in het Extranet worden gehasht en daar niet uit kunnen worden onttrokken. Verder voert Booking aan dat de getroffen accommodatie en de [VERTROUWELIJK] van Booking gezamenlijk tot de conclusie zouden zijn gekomen dat "het waarschijnlijk geen incident bij Booking was".

Voor wat betreft dit laatste, merkt de AP op dat naast het feit dat hiervoor geen onderbouwing is gegeven in de zienswijze, vast staat dat de [VERTROUWELIJK] van Booking niet heeft gehandeld volgens het eigen protocol van Booking, waarbij elk vermoeden van een incident direct dient te worden doorgezet aan het Security Team van Booking. De AP is van mening dat ondanks het gegeven dat e-mailadressen worden gehasht in het Extranet, voornoemd incident door Booking had moeten worden doorgezet aan het Security Team. Het feit dat de e-mail in kwestie immers de exacte reserveringsdetails van de betrokkene bevatte en het feit dat de boeking via het platform van Booking was gemaakt, hadden de [VERTROUWELIJK] van Booking moeten alarmeren en bewegen tot verdere actie.

Ten aanzien van het incident van 13 januari 2019 heeft Booking aangevoerd dat de [VERTROUWELIJK] in kwestie geen directe overeenkomsten zag met het eerdere incident waardoor niet met een redelijke mate van zekerheid zou kunnen worden gesteld dat zich bij Booking een veiligheidsincident had voorgedaan.

De AP is echter van oordeel dat het feit dat de (accommodatiemanager van de) Trip Provider reeds had afgewogen dat sprake was van een gelijkwaardig incident én het beveiligingsincident te maken moest hebben met het Extranet, waarvoor Booking verwerkingsverantwoordelijke is, maakt dat Booking op dat moment wel degelijk met een redelijke mate van zekerheid wist – en dus kennis had – dat zich een inbreuk in verband met persoonsgegevens had voorgedaan. Ook in dit geval waren de exacte reserveringsdetails van de betrokkene bekend bij een onbekende derde die zich valselijk voordeed als zijnde een medewerker van Booking. Op dit moment had Booking een redelijke mate van zekerheid van het beveiligingsincident waarbij persoonsgegevens waren gecompromitteerd. Het was in hoge mate zeker dat deze gegevens uit een door Booking ten behoeve van haar bedrijfsactiviteiten gebruikt platform waren verkregen, nu blijkens de e-mailcorrespondentie volgens de Trip Provider én de betrokkenen in kwestie kon worden uitgesloten dat zich aan hun zijde een beveiligingsincident had voorgedaan.

Schending interne meldplicht
Booking heeft verder aangevoerd dat het Booking niet mag worden tegengeworpen dat de procedure voor het melden van veiligheidsincidenten, die inhoudt dat veiligheidsincidenten door de Trip Providers via het zogenoemde "Partner Portal" bij het Security Team van Booking dienen te worden gemeld, door de accommodaties in kwestie[17] is geschonden. Volgens Booking mag het schenden van die meldplicht en het feit dat de [VERTROUWELIJK] van Booking niet onmiddellijke escaleerde niet aan Booking als onderneming worden tegengeworpen. Hierbij heeft Booking gewezen op een besluit van de Hongaarse privacy toezichthouder, die geoordeeld zou hebben dat nalatigheid vanuit slechts één deel van de organisatie niet aan de hele organisatie kan worden tegengeworpen indien passende maatregelen waren getroffen.[18]

[17] In casu de accommodaties in de Verenigde Arabische Emiraten.
[18] Boetebesluit Hungarian National Authority for Data Protection and Freedom of Information van 21 mei 2019, NAIH/2019/3854.

De AP stelt voorop dat op Booking als verwerkingsverantwoordelijke de verplichting rust om bij elk verontrustend signaal onderzoek te verrichten naar een eventuele inbreuk op de beveiliging van persoonsgegevens, zodat tijdig en in lijn met de bepalingen in de AVG kan worden gehandeld indien zich een inbreuk in verband met persoonsgegevens heeft voorgedaan. Dit staat volgens de AP los van eventuele privaatrechtelijke afspraken die Booking op dat punt eventueel gemaakt heeft met een derde partij, zoals in het onderhavige geval de betrokken Trip Providers. Uit paragraaf 5.1 van de door Booking overgelegde "Data Incident Response Policy" blijkt voorts dat ook alle vermoedens van incidenten, ook indien zij door "third party service providers" zoals de genoemde Trip Providers bij Booking zijn gemeld, direct dienen te worden doorgezet aan het Security Team van 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. (...)".*

Zowel op 9, 13 als 20 januari 2019 zijn door de accommodaties verschillende data-incidenten gemeld bij (de [VERTROUWELIJK] van) Booking, hetgeen echter niet heeft geleid tot de – in eigen procedures vastgelegde - vereiste melding daarvan bij het Security Team. Reeds op 13 januari 2019 was de [VERTROUWELIJK] van Booking op de hoogte van de inbreuk, desondanks is het Security Team pas op 31 januari 2019 op de hoogte gesteld.

Voor zover Booking met verwijzing naar het besluit van de Hongaarse toezichthouder een beroep heeft willen doen op het gelijkheidsbeginsel, merkt de AP op dat het in die zaak niet alleen gaat om een inbreuk van een geheel andere orde, namelijk een inbreuk op de vertrouwelijkheid van de persoonsgegevens door een zelfde organisatieonderdeel (van een overheidsorgaan) en niet om een geval van "social engineering" waarbij sprake is van een vorm van fraude, maar ook dat de AP in dat besluit een ander oordeel van de toezichthouder leest dan door Booking is geschetst. Het feit dat in die zaak te laat melding is gedaan van een inbreuk als bedoeld in artikel 33, eerste lid, van de AVG doordat een medewerker deze te laat had doorgezet wordt, anders dan Booking doet voorkomen, de organisatie in kwestie wel degelijk door de Hongaarse toezichthouder verweten.

Risico persoonlijke levenssfeer

Booking heeft voorts aangevoerd dat in het onderzoeksrapport ten onrechte een risico voor de persoonlijke levenssfeer is aangenomen zonder hierbij een analyse te maken van de door Booking geïmplementeerde beveiligingsmaatregelen gericht op het beschermen van de persoonlijke levenssfeer en het wegnemen van nadelige consequenties en heeft daarbij een aantal voorbeelden genoemd.[19]

[19] Genoemde voorbeelden: indien een datalek zich voordoet, blijft dit in het algemeen beperkt tot contactgegevens, zonder e-mailadressen, en reserveringsdata; creditcard gegevens worden opgeslagen volgens de PCI DSS normen; klanten worden ingelicht over social engineering en andere vormen van fraude; betrokkenen zijn onmiddellijk na het constateren van het datalek geïnformeerd en van advies gediend en Booking heeft aangegeven alle geleden schade te vergoeden.

De AP volgt laatstgenoemd standpunt van Booking niet. Zodra persoonsgegevens, zoals in dit geval, bij een daartoe onbevoegde persoon belanden en zijn ingezien, is reeds sprake van een risico voor de rechten en vrijheden van natuurlijke personen. Dit risico heeft zich in het onderhavige geval tevens geopenbaard nu betrokkenen benaderd waren door een onbekende derde die onrechtmatig over de persoonsgegevens van betrokkenen beschikte. Dat Booking nadien heeft toegezegd eventuele financiële schade te compenseren, doet niets af aan het feit dat de persoonsgegevens in verkeerde handen zijn beland. Het risico op eventuele gevolgen van de inbreuk is daarmee niet weggenomen.

Melding binnen 72 uur

Booking heeft verder aangevoerd dat het doen van een melding binnen 72 uur zoals bedoeld in artikel 33, eerste lid, van de AVG niet altijd mogelijk is. Het kan gespecialiseerde beveiligingsteams weken of maanden kosten om “data points” te verbinden en te concluderen dat een feitenpatroon inderdaad een datalek betreft dat moet worden gemeld. Verder zou het onjuist zijn en niet in overeenstemming met de AVG als de AP zou verwachten dat Booking in het algemeen slechts drie dagen nodig heeft om een onderzoek uit te voeren en kennis te nemen van een inbreuk in verband met persoonsgegevens. Daarnaast vermeldt de WP29 volgens Booking uitdrukkelijk in haar Richtsnoeren dat het wel even kan duren voordat een verwerkingsverantwoordelijke de omvang van de inbreuken kan vaststellen en de verwerkingsverantwoordelijke beter een zinvolle melding kan opstellen waarin meerdere, sterk op elkaar lijkende inbreuken worden gecombineerd dan elke inbreuk afzonderlijk te melden. Ten slotte heeft Booking aangevoerd dat in het onderzoeksrapport ten onrechte wordt overwogen dat Booking geen gegronde reden heeft gegeven voor de (vermeende) overtreding van de 72-uurs termijn. In de melding van 7 februari 2019 worden duidelijke redenen gegeven, gelegen in het grondige onderzoek door Booking, waarbij Booking herhaalt dat zij zich primair op het standpunt stelt dat melding is gedaan binnen 72 uur nadat zij bekend werd met de inbreuk in verband met persoonsgegevens.

De AP overweegt hieromtrent het volgende.

De AP onderschrijft het standpunt dat een onderzoek naar de omvang en precieze merites van een inbreuk langer dan 72 uur in beslag kan nemen. Omdat het niet altijd mogelijk is om te beschikken over alle noodzakelijke informatie over een inbreuk waardoor een melding kan worden gedaan die voldoet aan alle in het artikel 33, derde lid, van de AVG neergelegde vereisten, is de mogelijkheid tot het doen van een melding in stappen in de AVG opgenomen. Deze mogelijkheid is in artikel 33, vierde lid, van de AVG vastgelegd. Dit neemt niet weg dat de melding van de inbreuk op grond van artikel 33, eerste lid, van de AVG binnen de wettelijk voorgeschreven termijn van 72 uur moet plaatsvinden. Zoals in paragraaf 3.3.3 reeds opgemerkt moet Booking worden geacht op 13 januari 2019 kennis te hebben gekregen van de inbreuk in verband met persoonsgegevens. Dat de inbreuk op grond van artikel 33, eerste lid, van de AVG had moeten worden gemeld, was alsdan ook duidelijk. Booking heeft in het onderhavige geval te lang gewacht met het doen van de in artikel 33, eerste lid, van de AVG voorgeschreven melding. Het grondige onderzoek waar Booking naar verwijst rechtvaardigt geenszins de vertraging van vorenbedoelde (initiële) melding, waarmee dus sprake is van een onredelijke vertraging als bedoeld in artikel 33, eerste lid, van de AVG.

Zinvolle melding
Ten aanzien van hetgeen door Booking is aangevoerd met betrekking tot het opstellen van een zinvolle melding waarin meerdere op elkaar lijkende inbreuken gebundeld worden gemeld, overweegt de AP dat het er in de onderhavige zaak om draait dat Booking reeds op 13 januari 2019 kennis had van de inbreuk en de – al dan niet initiële – melding tijdig had moeten doen. Dat hier sprake zou zijn van meerdere op elkaar lijkende inbreuken die volgens Booking konden worden verpakt in één zinvolle melding acht de AP – gelet op hetgeen hiervoor, in paragraaf 3.4.3, is overwogen – niet relevant.

Rechtvaardiging vertraagde melding
Booking heeft aangevoerd dat buiten de Richtsnoeren geen instructies voorhanden zijn die aangeven met welke argumenten een vertraagde melding kan worden gerechtvaardigd en dat de AP een nieuwe norm niet met terugwerkende kracht kan toepassen. Bovendien had de AP kunnen vragen om de vertraging nader toe te lichten.

De AP overweegt hierover dat geen sprake is van het met terugwerkende kracht toepassen van een nieuwe norm. De in de AVG opgenomen regeling op dit punt is duidelijk: wanneer sprake is van een inbreuk in verband met persoonsgegevens moet deze zonder onredelijke vertraging, en indien mogelijk, uiterlijk 72 uur na kennisname bij de toezichthoudende autoriteit worden gemeld. De Richtsnoeren geven naar het oordeel van de AP duiding voor het voldoen aan de in de AVG opgenomen verplichting(en) tot het melden van inbreuken; ze zijn daarmee geenszins te beoordelen als een nieuwe norm. Overigens ligt het ten allen tijde op de weg van de verwerkingsverantwoordelijke om een melding die niet tijdig kan worden gedaan, te voorzien van een daarvoor toereikende motivering.

Praktische implicaties oordeel AP
Booking heeft in haar zienswijze voorts haar zorgen geuit over de volgens haar praktische implicaties van het oordeel van de AP in het onderzoeksrapport.[20] De daarin genoemde strikte uitleg brengt volgens Booking met zich mee dat alle potentiele beveiligingsincidenten, waarbij een kans bestaat dat persoonsgegevens worden gecompromitteerd, binnen 72 uur moeten worden gemeld en dat het Security Team elke klacht die bij Booking binnenkomt – ongeacht de wijze waarop en de inhoud daarvan – dient te onderzoeken. Dit zou naast een onredelijke en onrealistische administratieve belasting, tevens een onredelijke en onrealistische financiële belasting inhouden.[21] [VERTROUWELIJK]. Als alle individuele klachten meteen zouden moeten worden onderzocht zoals de AP voorstaat, zou aanzienlijk meer mankracht nodig zijn dan nu. Zulke onredelijke organisatorische maatregelen, met bijbehorende buitenproportionele uitvoeringskosten, druisen in tegen de gedachte achter de beveiligingsplicht van artikel 32 van de AVG, aldus Booking.

[20] In paragraaf 5 van de zienswijze.
[21] [VERTROUWELIJK]

De AP stelt voorop dat de AVG voorschrijft aan welke verplichtingen Booking in de hoedanigheid van verwerkingsverantwoordelijke moet voldoen. Op grond van artikel 32 van de AVG is een verwerkingsverantwoordelijke verplicht alle passende en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen: het vermogen om een inbreuk tijdig op te sporen, aan te pakken en te melden moet worden beschouwd als een essentieel onderdeel van deze maatregelen.[22] Volgens de AP vloeit niet uit het onderzoeksrapport voort dat elk potentieel beveiligingsincident zou moeten worden gemeld en dat elke klacht die bij Booking binnenkomt door het Security Team zou moeten worden onderzocht. Zodra een verwerkingsverantwoordelijke op de hoogte raakt van een beveiligingsincident of door een andere bron op de hoogte is gebracht van een mogelijke inbreuk, dient de verwerkingsverantwoordelijke te onderzoeken of sprake is van een meldplichtige inbreuk.[23] Uit de "Data Incident Response Policy" blijkt dat Booking haar beleid zo heeft ingericht dat vermoedens van en meldingen van vermeende beveiligingsincidenten direct ter beoordeling dienen te worden opgeschaald naar het Security Team. Dat dit in het onderhavige geval niet is gebeurd, komt naar het oordeel van de AP voor rekening en risico van Booking. Daarbij wijst de AP nogmaals op de situatie dat uit de verschillende meldingen van de accommodaties nagenoeg geen andere conclusie mogelijk was dan dat hier sprake was van een substantiële meldplichtige inbreuk.

Kennelijke verschrijving in rapport
Booking heeft aangevoerd dat het onderzoeksrapport in paragraaf 26 foutief 2 februari 2019 als datum noemt waarop het Security Team van Booking zijn bevindingen heeft vastgelegd maar dat die datum verder nergens in de stukken is genoemd. De AP gaat ervan uit dat hier sprake is van een kennelijke verschrijving nu in de stukken geen aanknopingspunt kan worden gevonden voor het gegeven dat het Security Team op 2 februari 2019 zijn bevindingen zou hebben gepresenteerd.

Ten overvloede
Hoewel dit verder in dit geval niet ter discussie staat, heeft Booking in de zienswijze aangegeven grote waarde te hechten aan gegevensbeveiliging en onmiddellijke actie op datalekken. Zij meent ruimschoots te voldoen aan de verwachtingen van artikel 34 van de AVG, en die zelfs te overtreffen, door betrokkenen over datalekken te informeren ook wanneer onwaarschijnlijk is dat een groot risico voor de rechten en vrijheden van de betrokkenen bestaat. De AP juicht dergelijke acties toe maar benadrukt dat dit Booking niet ontslaat van de overige in de AVG opgenomen verplichtingen, zoals de in artikel 33, eerste lid, van de AVG neergelegde meldplicht.

3.4.5 Conclusie
Gelet op het voorgaande is de AP van oordeel dat Booking artikel 33, eerste lid, van de AVG vanaf 16 januari 2019 tot en met 6 februari 2019 heeft overtreden, nu Booking de inbreuk in verband met persoonsgegevens niet tijdig, zonder onredelijke vertraging, bij de AP heeft gemeld.

[22] Zie Richtsnoeren p. 14/15.
[23] Zie hierover uitgebreid de Richtsnoeren van de WP29.

4. Boete

4.1 Inleiding

De AP maakt vanwege de hierboven vastgestelde overtreding gebruik van haar bevoegdheid om aan Booking een boete op te leggen op grond van artikel 58, tweede lid, aanhef en onder i en artikel 83, vierde lid, van de AVG, gelezen in samenhang met artikel 14, derde lid, van de UAVG. De AP hanteert hiervoor de Boetebeleidsregels 2019 (hierna: Boetebeleidsregels).[24]

In het hiernavolgende zal de AP eerst kort de boetesystematiek uiteenzetten, gevolgd door de motivering van de boetehoogte in het onderhavige geval.

4.2 Boetebeleidsregels Autoriteit Persoonsgegevens 2019 (Boetebeleidsregels 2019)

Ingevolge artikel 58, tweede lid, aanhef en onder i en artikel 83, vierde lid, van de AVG, gelezen in samenhang met artikel 14, derde lid, van de UAVG, is de AP bevoegd aan Booking in geval van een overtreding van artikel 33, eerste lid, van de AVG een bestuurlijke boete op te leggen tot € 10.000.000 of tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

De AP heeft Boetebeleidsregels vastgesteld inzake de invulling van voornoemde bevoegdheid tot het opleggen van een bestuurlijke boete, waaronder het bepalen van de hoogte daarvan.[25]

Ingevolge artikel 2, onder 2.1, van de Boetebeleidsregels 2019 zijn de bepalingen ter zake van overtreding waarvan de AP een bestuurlijke boete kan opleggen van ten hoogste het bedrag van € 10.000.000 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, in bijlage 1 ingedeeld in categorie I, categorie II of categorie III.

In bijlage 1 is artikel 33, eerste lid, van de AVG ingedeeld in categorie III.

Ingevolge artikel 2, onder 2.3, stelt de AP de basisboete voor overtredingen ingedeeld in categorie III vast binnen de volgende boetebandbreedte: € 300.000 en € 750.000 en een basisboete van € 525.000.

Ingevolge artikel 6 bepaalt de AP de hoogte van de boete door het bedrag van de basisboete naar boven (tot ten hoogste het maximum van de bandbreedte van de aan een overtreding gekoppelde boetecategorie) of naar beneden (tot ten laagste het minimum van die bandbreedte) bij te stellen. De basisboete wordt verhoogd of verlaagd afhankelijk van de mate waarin de factoren die zijn genoemd in artikel 7 daartoe aanleiding geven.

Ingevolge artikel 7 houdt de AP onverminderd de artikelen 3:4 en 5:46 van de Algemene wet bestuursrecht

[24] Stcrt. 2019, 14586, 14 maart 2019.
[25] Stcrt. 2019, 14586, 14 maart 2019.

(Awb) rekening met de factoren die zijn ontleend aan artikel 83, tweede lid, van de AVG, in de Beleidsregels genoemd onder a tot en met k:
a. de aard, de ernst en de duur van de inbreuk, rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade;
b. de opzettelijke of nalatige aard van de inbreuk;
c. de door de verwerkingsverantwoordelijke [...] genomen maatregelen om de door betrokkenen geleden schade te beperken;
d. de mate waarin de verwerkingsverantwoordelijke [...] verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd overeenkomstig de artikelen 25 en 32 van de AVG;
e. eerdere relevante inbreuken door de verwerkingsverantwoordelijke [...];
f. de mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;
g. de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft;
h. de wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke [...] de inbreuk heeft gemeld;
i. de naleving van de in artikel 58, tweede lid, van de AVG genoemde maatregelen, voor zover die eerder ten aanzien van de verwerkingsverantwoordelijke [...] in kwestie met betrekking tot dezelfde aangelegenheid zijn genomen;
j. het aansluiten bij goedgekeurde gedragscodes overeenkomstig artikel 40 van de AVG of van goedgekeurde certificeringsmechanismen overeenkomstig artikel 42 van de AVG; en
k. elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende factor, zoals gemaakte financiële winsten, of vermeden verliezen, die al dan niet rechtstreeks uit de inbreuk voortvloeien.

Ingevolge artikel 9 van de Boetebeleidsregels 2019 houdt de AP bij het vaststellen van de boete zo nodig rekening met de financiële omstandigheden waarin de overtreder verkeert. In geval van verminderde of onvoldoende draagkracht van de overtreder kan de AP de op te leggen boete verdergaand matigen, indien, na toepassing van artikel 8.1 van de beleidsregels, vaststelling van een boete binnen de boetebandbreedte van de naast lagere categorie naar haar oordeel desalniettemin zou leiden tot een onevenredig hoge boete.

4.3 Boetehoogte

4.3.1. Aard, ernst en duur van de inbreuk

Ingevolge artikel 7, aanhef en onder a, van de Boetebeleidsregels houdt de AP rekening met de aard, de ernst en de duur van de inbreuk. Bij de beoordeling hiervan betrekt de AP onder meer de aard, de omvang of het doel van de verwerking alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade.

De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht. Krachtens artikel 8, eerste lid, van het Handvest van de grondrechten van de Europese Unie en artikel 16, eerste lid, van het Verdrag betreffende de werking van de Europese Unie (VWEU) heeft eenieder recht op

bescherming van zijn persoonsgegevens. De beginselen en regels betreffende de bescherming van natuurlijke personen bij de verwerking van hun persoonsgegevens dienen in overeenstemming te zijn met hun grondrechten en fundamentele vrijheden, met name met hun recht op bescherming van persoonsgegevens. De AVG beoogt bij te dragen aan de totstandkoming van een ruimte van vrijheid, veiligheid en recht en van een economische unie, alsook tot economische en sociale vooruitgang, de versterking en de convergentie van de economieën binnen de interne markt en het welzijn van natuurlijke personen. De verwerking van persoonsgegevens moet ten dienste van de mens staan. Het recht op bescherming van persoonsgegevens heeft geen absolute gelding, maar moet worden beschouwd in relatie tot de functie ervan in de samenleving en moet conform het evenredigheidsbeginsel tegen andere grondrechten worden afgewogen. Elke verwerking van persoonsgegevens dient behoorlijk en rechtmatig te geschieden. De persoonsgegevens dienen toereikend en ter zake dienend te zijn en beperkt te blijven tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Persoonsgegevens moeten worden verwerkt op een manier die een passende beveiliging en vertrouwelijkheid van die gegevens waarborgt, ook ter voorkoming van ongeoorloofde toegang tot of het ongeoorloofde gebruik van persoonsgegevens en de apparatuur die voor de verwerking wordt gebruikt.

De melding van inbreuken moet worden gezien als een middel om de naleving van de regels in verband met de bescherming van persoonsgegevens te verbeteren. Indien een inbreuk in verband met persoonsgegevens plaatsvindt of heeft plaatsgevonden, kan dit resulteren in lichamelijke, materiele of immateriële schade voor natuurlijke personen of enig ander economisch of maatschappelijk nadeel voor de persoon in kwestie. Daarom dient de verwerkingsverantwoordelijke, zodra hij weet heeft gekregen van een inbreuk in verband met persoonsgegevens de toezichthouder onverwijld en zo mogelijk binnen 72 uur in kennis stellen van de inbreuk in verband met persoonsgegevens. De toezichthouder wordt daarmee in staat gesteld om haar taken en bevoegdheden, zoals neergelegd in de AVG, op goede wijze uit te voeren.

Booking heeft niet alleen nagelaten de inbreuk in verband met persoonsgegevens onverwijld te melden, maar heeft op meerdere momenten, te weten op 9, 13 en 20 januari 2019, terwijl onverwijlde actie had mogen worden verwacht, stilgezeten waardoor sprake is van een (zeer) onredelijke vertraagde melding bij de AP. Voorts is gebleken dat Booking in plaats van het doen van een melding in stappen, er bewust voor heeft gekozen om eerst een grondig onderzoek te verrichten, alvorens het doen van de vereiste melding bij de toezichthoudende autoriteit. Dit is niet in lijn met de regeling zoals neergelegd in de AVG.

Uit het door het Security Team van Booking verrichtte onderzoek is gebleken dat mogelijk 4109 betrokkenen zijn getroffen. Dit waren hotelgasten, die via het platform van Booking hotelovernachtingen, bij 40 verschillende accommodaties, hadden gereserveerd. Door middel van het plegen van “social engineering” fraude zijn naast NAW-gegevens en gegevens betreffende hotelreserveringen ook creditcard gegevens bij onbevoegde derden terechtgekomen. Dit zijn gevoelige gegevens die in handen van onbevoegden tot financieel dan wel ander nadeel kunnen leiden.

Gelet op de aard van de persoonsgegevens, het aantal persoonsgegevens, het aantal getroffen betrokkenen, de duur van de overtreding alsmede het belang van een tijdige melding aan de toezichthouder binnen 72

uur, is naar het oordeel van de AP sprake van een ernstige overtreding, maar de AP ziet in dit geval geen aanleiding om het basisboetebedrag te verhogen of te verlagen.

4.3.2 Opzettelijke of nalatige aard van de inbreuk (verwijtbaarheid)

Ingevolge artikel 5:46, tweede lid, van de Awb houdt de AP bij de oplegging van een bestuurlijke boete rekening met de mate waarin deze aan de overtreder kan worden verweten. Ingevolge artikel 7, onder b, van de Boetebeleidsregels 2019 houdt de AP rekening met de opzettelijke of nalatige aard van de inbreuk.

Artikel 33, eerste lid, van de AVG schrijft voor dat een inbreuk in verband met persoonsgegevens zonder onredelijke vertraging dient te worden gemeld en, indien mogelijk, uiterlijk 72 uur nadat de verwerkingsverantwoordelijke daarvan kennis heeft genomen. Een meldplicht als zodanig kent Nederland reeds sinds 1 januari 2016, toen deze norm werd geïntroduceerd in de Wet bescherming persoonsgegevens (Wbp).[26]
De AP stelt zich ten aanzien van de kennis, die een normadressaat, zoals in dit geval Booking, van de toepasselijke wet- en regelgeving geacht wordt te hebben, op het standpunt dat als uitgangspunt heeft te gelden dat marktpartijen een eigen verantwoordelijkheid dragen om zich aan de wet te houden.[27]
De AP heeft marktpartijen ook ruimschoots voorgelicht over de toepasselijke wet- en regelgeving, zodat verondersteld mag worden dat ook Booking hiermee bekend was. Daarnaast is in de media uitvoerig aandacht besteed aan de meldplicht datalekken.

Uit het hierboven weergegeven wettelijk kader in samenhang met de toepasselijke richtsnoeren van de WP29, waar Booking reeds voor de inbreuk kennis van had kunnen nemen, volgt naar het oordeel van de AP voldoende duidelijk dat Booking de inbreuk tijdig aan de AP had moeten melden en dat dit zonder onredelijke vertraging, maar in elk geval uiterlijk binnen 72 uur na 13 januari 2019 had moeten geschieden. Bovendien had de melding aan de AP voorwaardelijk kunnen worden gedaan, in de zin dat de melding naderhand zou kunnen worden aangevuld. Die mogelijkheid wordt in de AVG uitdrukkelijk geboden. Indien twijfel had gerezen over de reikwijdte van het gebod dan heeft, ook volgens vaste rechtspraak, te gelden dat van een professionele en multinationaal opererende marktpartij als Booking mag worden verlangd dat deze zich terdege informeert of laat informeren over de beperkingen waaraan haar gedragingen zijn onderworpen, zodat zij haar gedrag van meet af aan had kunnen afstemmen op de reikwijdte van dat gebod.[28]

Het disculpeert Booking als zelfstandig drager van rechten en plichten naar het oordeel van de AP niet dat een [VERTROUWELIJK] van Booking in strijd heeft gehandeld met het eigen protocol van Booking dat voorschrijft elk vermoeden van een incident direct ter beoordeling door te zetten aan het Security Team. Dit is toe te rekenen aan Booking.

[26] In artikel 34a, eerste lid, van de Wbp.
[27] Vgl. CBb 25 juni 2013, ECLI:NL:CBB:2013:4, r.o. 2.3, CBb 25 januari 2017, ECLI:NL:CBB:2017:14, r.o. 5.2, CBb 8 maart 2017, ECLI:NL:CBB:2017:91, r.o. 6.
[28] Vgl. CBb 22 februari 2012, ECLI:NL:CBB:2012:BV6713, r.o. 4.3, CBb 19 september 2016, ECLI:NL:CBB:2016:290, r.o. 8.6., CBb 19 september 2016, ECLI:NL:CBB:2016:372, r.o. 6.3.

Booking heeft 22 dagen te laten gemeld. De AP acht dit verwijtbaar. De AP ziet evenwel geen aanleiding om het basisbedrag van de boete op grond van artikel 7, onder b, van de Boetebeleidsregels 2019 te verhogen of te verlagen.

4.3.3 Schadebeperkende maatregelen

Ingevolge artikel 7, onder c, van de Boetebeleidsregels 2019 houdt de AP rekening met de door de verwerkingsverantwoordelijke genomen maatregelen om de door betrokkenen geleden schade te beperken.

Booking heeft in haar zienswijze naar voren gebracht diverse concrete herstelacties te hebben ondernomen om eventuele schade voor betrokkenen te beperken. Zo heeft Booking betrokkenen ingelicht en geadviseerd over het nemen van schadebeperkende maatregelen. Verder heeft Booking zich bereid verklaard eventuele door betrokkenen (geleden of nog te lijden) schade te vergoeden. Ten slotte heeft Booking de getroffen accommodaties onmiddellijk ingelicht en waarschuwingen op het platform van Booking geplaatst.

De AP is van mening dat hoewel Booking heeft nagelaten de inbreuk op tijd te melden bij de toezichthouder, het Booking siert dat zij genoemde maatregelen heeft getroffen en zich bereid heeft verklaard eventuele schade te vergoeden. Het feit dat Booking op dit punt uiteindelijk voortvarend heeft opgetreden, waardoor de schadelijke gevolgen voor betrokkenen hoogstwaarschijnlijk beperkt zijn gebleven, weegt de AP mee bij het bepalen van de boetehoogte.

Gezien de door Booking naar aanleiding van de inbreuk getroffen maatregelen om de schade voor betrokkenen te beperken, ziet de AP aanleiding om het basisbedrag van de boete op grond van artikel 7, onder c, van de Boetebeleidsregels 2019 te verlagen met € 50.000.

4.3.4 Overige omstandigheden

De AP ziet voorts geen aanleiding het basisbedrag van de boete op grond van de overige in artikel 7 van de Boetebeleidsregels 2019 genoemde omstandigheden, voor zover van toepassing in het voorliggende geval, te verhogen of te verlagen.

De AP stelt het boetebedrag inzake overtreding van artikel 33, eerste lid, van de AVG gelet op de in artikel 7 van de AVG genoemde factoren vast op € 475.000.

4.3.5 Zienswijze Booking en reactie AP

Booking heeft ten aanzien van het opleggen van een bestuurlijke boete in haar zienswijze primair aangevoerd dat het opleggen van een bestuurlijke boete niet evenredig zou zijn. Door Booking is daarbij verwezen naar boetes die voor overtredingen van artikel 33, eerste lid, van de AVG zijn opgelegd door de Litouwse, Hongaarse en Hamburgse Autoriteit.[29] Booking stelt zich op het standpunt dat in het kader van

[29] Paragraaf 9.2, onder a, van de zienswijze.

het idee van harmonisatie voor soortgelijke overtredingen binnen Europa gelijke boetes dienen te worden opgelegd.

Momenteel zijn op Europees niveau geen gezamenlijke uitgangspunten voor de berekening van boetebedragen overeen gekomen. Zodoende hanteert de AP zelfstandig de door haar vastgestelde Boetebeleidsregels voor de berekening van boetebedragen. Bovendien beoordeelt de AP deze zaak op zijn eigen merites en dus naar de specifieke feiten en omstandigheden van deze zaak. Het hoeft geen betoog dat deze per zaak verschillend zijn en daarmee niet met elkaar vergelijkbaar. Tot slot zijn de door Booking in haar zienswijze naar voren gebrachte boetebesluiten van andere privacy toezichthouders niet tot stand gekomen via het zogenoemde coherentiemechanisme, zoals neergelegd in hoofdstuk 7 van de AVG, en is de AP zodoende reeds daarom niet gebonden aan die beslissingen en niet gehouden om in de onderhavige zaak een boete van gelijke hoogte op te leggen.

Booking heeft daarnaast aangevoerd dat het opleggen van een bestuurlijke boete in strijd zou zijn met het lex certa-beginsel, omdat duidelijke richtsnoeren van de AP en het Europees Comité voor Gegevensbescherming voor het motiveren van een vertraagde melding van een datalek ontbreken.

De AP deelt ook dit standpunt van Booking niet en verwijst hiervoor naar hetgeen in paragrafen 3.4.4 en 4.3.2 van dit besluit is overwogen.

Ten slotte heeft Booking (meer) subsidiair aangevoerd dat indien de AP toch besluit om een boete op te leggen, deze op grond van artikel 6 jo. 8.1 van de Boetebeleidsregels dient te worden verlaagd naar de laagste boete in categorie II.

Met betrekking tot de aard, ernst en duur van de overtreding heeft Booking kort gezegd aangevoerd dat de door Booking genomen preventieve en corrigerende maatregelen het aantal getroffen personen en de omvang van de schade hebben beperkt.

De AP ziet, onder verwijzing naar paragraaf 4.3.1, op basis hiervan geen aanleiding af te zien van het opleggen van een bestuurlijke boete of het boetebedrag te verlagen.

Ten aanzien van de opzettelijke of nalatige aard van de inbreuk heeft Booking aangevoerd dat de overtreding niet volgt uit enig opzet of nalatigheid zijdens Booking en verwijst hiervoor naar de technische en organisatorische maatregelen die zijn getroffen ter voorkoming van ‘social engineering’ incidenten en ter beperking van gevolgen.

De AP wijst dit standpunt van de hand. Zoals in paragraaf 4.3.2 is neergelegd, is de AP van mening dat sprake is van een nalatigheid die valt toe te rekenen aan Booking. De AP ziet hierin geen aanleiding het basis boetebedrag te verhogen of te verlagen.

Met betrekking tot de genomen maatregelen om de schade te beperken stelt Booking dat de technische en organisatorische maatregelen die zij heeft getroffen passend zijn en mogelijk zelfs de vereisten van de AVG overtreffen.

Zoals hiervoor in paragraaf 4.3.3 aan de orde is gekomen, ziet de AP hierin aanleiding het basisboetebedrag te verlagen.

Ten aanzien van de mate van verantwoordelijkheid gezien de door Booking op grond van de artikelen 25 en 32 van de AVG getroffen technische en organisatorische maatregelen heeft Booking aangevoerd dat de systemen en organisatie van Booking zodanig zijn opgezet dat de beginselen van gegevensbescherming doeltreffend kunnen worden geïmplementeerd, waarbij Booking herhaalt dat zij gezien de getroffen maatregelen en de aard van het incident niet aansprakelijk kan worden gesteld voor het datalek en de vermeende overtreding.

De AP deelt dit standpunt niet. Van een professionele partij als Booking mag, mede gelet op de aard en de omvang van de verwerking, worden verwacht dat zij zich terdege van de voor haar geldende normen vergewist en deze naleeft. Zoals eerder overwogen in paragraaf 4.3.2 van dit besluit is Booking ten volle verantwoordelijk te houden voor de overtreding. Daarom ziet de AP ook hierin geen aanleiding de boete te verlagen.

Met betrekking tot eerdere relevante inbreuken op de AVG heeft Booking aangevoerd dat zij geen eerdere berichten van de AP heeft ontvangen over vermeende overtredingen van artikel 33, eerste lid, van de AVG.

De AP ziet niet in waarom dit standpunt van Booking zou moeten leiden tot een vermindering van het basisboetebedrag. Het feit dat de AP Booking niet eerder heeft aangeschreven voor een identieke overtreding leidt niet tot de vaststelling dat een verlaging van het boetebedrag in aanmerking komt. [VERTROUWELIJK]

Ten aanzien van de samenwerking tussen Booking en de AP teneinde de vermeende overtreding te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken, heeft Booking aangevoerd dat zij volledige medewerking heeft verleend aan de AP door tijdig alle vragen te beantwoorden en indien door de AP om een nadere verklaring van de vertraging van de melding had gevraagd, zou deze verklaring zijn gegeven.

De AP ziet hierin geen aanleiding tot het verlagen van het boetebedrag. De AP is van oordeel dat de medewerking van Booking niet verder is gegaan dan haar wettelijke plicht om te voldoen aan artikel 33, eerste lid, van de AVG. Booking heeft daarmee niet op bijzondere wijze samengewerkt met de AP.

Ten aanzien van de overige factoren heeft Booking kort gezegd aangevoerd dat de gegevens geen betrekking hebben op bijzondere categorieën van persoonsgegevens of een kwetsbare groep personen, Booking volledig transparant naar betrokkenen en de AP is geweest en het datalek zelf bij de AP heeft gemeld. Ten slotte heeft Booking aangevoerd dat indien zij haar melding eerder aan de AP had gedaan, dit

niet zou hebben geleid tot andere maatregelen zijdens Booking of verdere beperking van de risico's voor de persoonlijke levenssfeer van betrokkenen. Geen enkele betrokkene heeft enigerlei nadeel ondervonden door het tijdstip van de melding, aldus Booking.

Ook hierin volgt de AP de zienswijze van Booking niet. Ondanks het feit dat de inbreuk, voor zover wij weten, geen bijzondere persoonsgegevens heeft getroffen, Booking zelfstandig betrokkenen heeft geïnformeerd en de (financiële) gevolgen voor betrokkenen beperkt zijn gebleven, ziet de AP door de ernst van de overtreding en de verwijtbaarheid van Booking geen aanleiding om het boetebedrag verder te verlagen. De AP verwijst voor de motivering hiervan naar paragrafen 4.3.1 en 4.3.2.

4.3.6 Evenredigheid en wettelijk boetemaximum

Tot slot beoordeelt de AP op grond van artikelen 3:4 en 5:46 van de Awb (evenredigheidsbeginsel) of de toepassing van haar beleid voor het bepalen van de hoogte van de boete gezien de omstandigheden van het concrete geval, niet tot een onevenredige uitkomst leidt. Toepassing geven aan het evenredigheidsbeginsel brengt volgens de Boetebeleidsregels 2019 mee dat de AP bij het vaststellen van de boete zo nodig rekening houdt met de financiële omstandigheden waarin de overtreder verkeert.

Gelet op al wat hiervoor is overwogen, is de AP van oordeel dat de hoogte van de op te leggen boete niet tot een onevenredige uitkomst leidt. Daarnaast is het onderhavige besluit tot stand gekomen via het in de AGV voorgeschreven coherentiemechanisme. De overige (betrokken) toezichthouders in Europa hebben het oordeel van de AP onderschreven.

De AP ziet geen aanleiding om aan te nemen dat Booking een boete van € 475.000,-- gezien haar financiële positie niet zou kunnen dragen.

4.4 Conclusie

De AP stelt het totale boetebedrag vast op € 475.000.

Datum
10 december 2020

Ons kenmerk
[VERTROUWELIJK]

5. Dictum

Boete

De AP legt aan Booking, wegens overtreding van artikel 33, eerste lid, van de AVG een bestuurlijke boete op ten bedrage van **€ 475.000,--** (zegge: vierhonderdvijfenzeventigduizend euro).[30]

Hoogachtend,
Autoriteit Persoonsgegevens,

drs. C.E. Mur
Bestuurslid

Rechtsmiddelenclausule
Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens.
Ingevolge artikel 38 van de UAVG schort het indienen van een bezwaarschrift de werking van de beschikking tot oplegging van de bestuurlijke boete op.
Voor het indienen van digitaal bezwaar, zie www.autoriteitpersoonsgegevens.nl, onder het kopje Bezwaar maken tegen een besluit, onderaan de pagina onder de kop Contact met de Autoriteit Persoonsgegevens.
Het adres voor het indienen op papier is: Autoriteit Persoonsgegevens, postbus 93374, 2509 AJ Den Haag.
Vermeld op de envelop 'Awb-bezwaar' en zet in de titel van uw brief 'bezwaarschrift'.
Schrijf in uw bezwaarschrift ten minste:
- uw naam en adres;
- de datum van uw bezwaarschrift;
- het in deze brief genoemde kenmerk (zaaknummer); of een kopie van dit besluit bijvoegen;
- de reden(en) waarom u het niet eens bent met dit besluit;
- uw handtekening.

[30] De AP zal voornoemde vordering uit handen geven aan het Centraal Justitieel Incassobureau (CJIB).