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

Vertrouwelijk/Aangetekend
Transavia Airlines C.V.
t.a.v. de directie
Piet Guilonardweg 15
1117 EE Schiphol

Datum
23 september 2021

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Besluit tot het opleggen van een boete

Geachte heer, mevrouw,

De Autoriteit Persoonsgegevens (AP) heeft besloten om aan Transavia Airlines C.V. een **bestuurlijke boete** van **€ 400.000** op te leggen. De AP komt is tot de conclusie gekomen dat Transavia geen passende maatregelen getroffen heeft om een op het risico afgestemd beveiligingsniveau te waarborgen. Hierdoor heeft Transavia in strijd gehandeld met artikel 32, eerste en tweede lid, van de Algemene verordening gegevensbescherming.

De AP licht het besluit hierna nader toe. Hoofdstuk 1 betreft een inleiding en hoofdstuk 2 bevat de feiten. De AP beoordeelt in hoofdstuk 3 of er sprake is van verwerking van persoonsgegevens, 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.

Datum
23 september 2021

Ons kenmerk
[VERTROUWELIJK]

1. Inleiding

1.1 Betrokken organisatie

Dit besluit heeft betrekking op Transavia Airlines C.V. (hierna: Transavia), gevestigd aan de Piet Guilonardweg 15, 1117 EE te Schiphol. Het bedrijf staat ingeschreven in het handelsregister onder nummer: 34069081.[1] Als luchtvaarmaatschappij verzorgt Transavia vluchten voor zakelijke reizigers en consumenten binnen Europa.

Op 24 oktober 2019 heeft de AP een melding ontvangen van Transavia over een inbreuk op de beveiliging van persoonsgegevens als bedoeld in artikel 33 van de AVG. In deze melding is door Transavia aangegeven dat een kwaadwillende derde partij ongeautoriseerd toegang heeft gehad tot systemen van Transavia. Naar aanleiding hiervan heeft de AP ambtshalve onderzocht of de technische maatregelen bij Transavia met betrekking tot de toegang tot persoonsgegevens passend waren als bedoeld in artikel 5, lid 1, sub f jo. artikel 32 van de AVG. Specifiek richtte dit onderzoek zich op de toegang tot bepaalde gebruikers-accounts bij Transavia, alsmede de rechten en mogelijkheden die deze gebruikers-accounts hadden binnen de systemen van Transavia.

1.2 Procesverloop

Op 28 november 2019 heeft de AP telefonisch contact opgenomen met Transavia over de datalekmelding van 24 oktober 2019 en de daarop volgende meldingen. Toezichthouders van de AP hebben vervolgens meermaals informatie opgevraagd bij Transavia waarop Transavia deze informatie heeft geleverd.

Bij brief van 12 mei 2021 heeft de AP aan Transavia een voornemen tot handhaving verzonden en het daaraan ten grondslag gelegde rapport met bevindingen. Transavia heeft op 28 juni 2021 hierop schriftelijk een zienswijze gegeven.

[1] Zie Dossierstuk 26, Inschrijving Handelsregister Transavia Airlines C.V.

2. Feiten

2.1 De inbreuk bij Transavia

In de datalekmelding van 24 oktober 2019 heeft Transavia aangegeven dat een kwaadwillende derde partij (hierna ook: 'aanvaller') ongeautoriseerd toegang heeft gehad tot systemen van Transavia.[2] Transavia is volgens de melding hier op 21 oktober 2019 achter gekomen. Transavia heeft vervolgens een externe dienstverlener ingeschakeld en samen met deze dienstverlener is de aanvaller van de systemen van Transavia geweerd. Verder heeft de externe dienstverlener geanalyseerd welke systemen getroffen waren en welke gegevens betrokken waren.

In het rapport opgesteld door de externe dienstverlener (hierna ook: 'forensisch rapport') is beschreven dat een aanvaller gebruik heeft gemaakt van [VERTROUWELIJK] e-mailadressen. Deze adressen zijn mogelijk te vinden op het internet.[3] De aanvaller probeerde toegang te verkrijgen tot de [VERTROUWELIJK][4]

De aanvaller heeft gebruik gemaakt van een "*password spray*" of "*credential stuffing*" aanval. Met een "*password spray*" aanval gebruikt een aanvaller veel gebruikte wachtwoorden om op een geautomatiseerde manier ongeautoriseerde toegang te krijgen. Bij "*credential stuffing*" aanval gebruikt een aanvaller bekende gebruikersgegevens (afkomstig uit andere datalekken van derden) om te proberen toegang te krijgen tot een systeem.

Op 12 september 2019 om 9:52 uur vond een succesvolle inlogpoging plaats door de aanvaller. De gebruikte gebruikersnaam was [VERTROUWELIJK] en het wachtwoord was [VERTROUWELIJK]. Met deze inlog kon de aanvaller gebruikmaken van de [VERTROUWELIJK] gebruiker.[5] Dit is een gebruiker die werd gebruikt voor [VERTROUWELIJK].[6]

Met de [VERTROUWELIJK] gebruiker was het mogelijk om toegang te krijgen tot een Citrix omgeving van Transavia. Citrix is software die het mogelijk maakt om te telewerken. Vervolgens was het mogelijk om mogelijke [VERTROUWELIJK]-gebruikers in het [VERTROUWELIJK] domein te achterhalen.[7]

Het is de aanvaller vervolgens gelukt om de authenticatiegegevens te verkrijgen van de gebruiker [VERTROUWELIJK] door wederom het wachtwoord [VERTROUWELIJK] te gebruiken. Deze gebruiker

[2] Transavia France S.A.S. (zustermaatschappij van Transavia) heeft afzonderlijk gemeld bij de Franse toezichthouder volgens de datalekmelding van 24 oktober 2019 omdat er ook persoonsgegevens zouden zijn betrokken waar Transavia France S.A.S verantwoordelijk voor is. Zie Dossierstuk 1, melding van 24 oktober 2019.
[3] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 21.
[4] Active Directory Federation Services Webservice is software van Microsoft, die organisaties in staat stelt Single Sign On Services te bewerkstellingen in een organisatie.
[5] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 21.
[6] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[7] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 21. Een netwerkdomein is een groep computers (systemen) binnen een computernetwerk met als doel de systemen gecentraliseerd te beheren.

had volgens Transavia "*de hoogste privileges in het* [VERTROUWELIJK]".[8] In principe betekent dit dat de accounts [VERTROUWELIJK] en [VERTROUWELIJK] tezamen toegang verschaften tot een groot deel van het computernetwerk van Transavia.[9] De rol van het account was bedoeld om te dienen als koppeling tussen het HR systeem van Transavia en de Active Directory (om te bepalen welke medewerkers welke rechten tot systemen behoren te krijgen).[10] Active Directory is een dienst van Microsoft die (onder andere) wordt gebruikt om rechten van gebruikers te beheren.

Vervolgens verkende de aanvaller de systemen van Transavia die onderdeel zijn van het domein. In deze verkenningsfase, is er (waarschijnlijk geautomatiseerd) ingelogd op [VERTROUWELIJK] systemen.[11] In totaal is er activiteit waargenomen betreffende [VERTROUWELIJK] systemen. De externe dienstverlener heeft op [VERTROUWELIJK] systemen vast kunnen stellen dat sprake is van gegevens die zijn gekopieerd.[12] De aanvaller had mogelijk interesse in toegang tot [VERTROUWELIJK]. Toegang hiertoe verkrijgen is echter niet gelukt.[13] Dit is ook bevestigd door Transavia.[14]

De aanvaller heeft op tenminste [VERTROUWELIJK] systemen [VERTROUWELIJK] logbestanden verwijderd.[15]

De aanvaller heeft verder gebruik gemaakt van [VERTROUWELIJK] software. Dit is penetratie test software die bedoeld is om kwetsbaarheden te vinden in een IT-landschap. De externe dienstverlener heeft op tenminste [VERTROUWELIJK] systemen hier aanwijzingen voor gevonden. Op 21 oktober 2019 is dit type aanval door de beheerder opgemerkt en heeft de beheerder onderzoek ingesteld. Na 21 oktober 2019 zijn ook geen activiteiten meer waargenomen van de aanvaller.[16]

Op basis van deze signalering is door Transavia op 22 oktober 2019 een externe dienstverlener ingeschakeld (niet de beheerder). De externe dienstverlener heeft een forensische analyse uitgevoerd. Uit de analyse bleek dat het merendeel van de activiteiten van de aanvaller gericht waren op verkenningsactiviteiten. De volgende gegevens zijn echter wel gekopieerd: Netwerk documentatie, zakelijke en diverse andere documenten alsmede zes e-mailboxen.[17]

Er zijn door Transavia [VERTROUWELIJK] systemen als kritiek bestempeld. Hier zat een systeem tussen voor de uitwisseling van gegevens met [VERTROUWELIJK]. Ook zaten hier [VERTROUWELIJK] bij en een [VERTROUWELIJK]. Op een van de kritieke systemen, het [VERTROUWELIJK], zijn bepaalde logbestanden verwijderd. Hierdoor was er op dit systeem minder bewijs over wat er gebeurd is met dit systeem.[18]

[8] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.
[9] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 21.
[10] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[11] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 21.
[12] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 26.
[13] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 25.
[14] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[15] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 23.
[16] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 25.
[17] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 4.
[18] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 17.

Op 22 november 2019 heeft Transavia opdracht gegeven aan de externe dienstverlener om de mailboxen te onderzoeken die door de aanvaller in deze inbreuk zijn gekopieerd naar een externe locatie. Het doel van het onderzoek betrof de persoonsgegevens in zes mailboxen: vijf mailboxen van medewerkers en één van een oud-medewerker. In de mailboxen bleken 49 bestanden met persoonsgegevens aanwezig.[19] Deze mailboxen waren volgens Transavia (met name) in gebruik bij [VERTROUWELIJK] medewerkers.[20]

Deze bestanden zijn vervolgens geanalyseerd en op basis hiervan is besloten een mededeling te doen aan 81.000 betrokkenen, zoals verplicht in artikel 34 van de AVG indien er mogelijk sprake is van een hoog risico.[21] Deze groep betrokkenen bestond uit werknemers van Transavia en klanten van Transavia. De medewerkers wiens mailboxen waren gekopieerd, waren reeds mondeling geïnformeerd volgens Transavia.[22]

Transavia geeft aan dat sinds 25 november 2019 de aanvaller definitief geen toegang meer had tot het IT-landschap van Transavia.[23] Dit is ook bevestigd door de externe dienstverlener.[24]

Samenvattend heeft een onbevoegde derde partij toegang gehad tot systemen van Transavia. Bij deze toegang was het mogelijk een gebruiker met veel rechten te gebruiken, waardoor de aanvaller veel mogelijkheden had binnen deze systemen. Hierdoor is er toegang geweest tot veel systemen en zijn er ook persoonsgegevens gekopieerd naar een externe locatie.

2.2 Soort persoonsgegevens

Er zijn twee groepen te onderscheiden persoonsgegevens in deze inbreuk: (1) persoonsgegevens die de aanvaller heeft gekopieerd naar een externe locatie en (2) persoonsgegevens waar de aanvaller toegang tot had.

2.2.1 Persoonsgegevens die zijn gekopieerd naar een externe locatie

De volgende persoonsgegevens die zich in de mailboxen bevonden zijn door de aanvaller gekopieerd (exclusief de bestandsnamen):[25]

[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]

[19] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020 – Bijlage 2: Onderzoeksrapport mailboxen.
[20] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[21] Dossierstuk 13, Persbericht Transavia.
[22] Dossierstuk 2, Vervolgmelding van 22 november 2019.
[23] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[24] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 4.
[25] Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020 – Bijlage 3: Toelichting bij bijlage 2.

[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]

Uit de bovenstaande tabel blijkt dat zowel passagiers-, leveranciers- en (potentiele) werknemersgegevens zijn gekopieerd. Transavia heeft verklaard dat het hier circa 80.000 passagiers betreft.[26] Ook stonden in meerdere bestanden de persoonsgegevens van tot 3000 medewerkers en tot 200 leveranciers.[27]

Van passagiers zijn betrokken: voor- en achternaam, geboortedatum, vluchtinformatie en SSR-code. Van één passagier is een adres en telefoonnummer betrokken. Van medewerkers gaat het om de volgende gegevens: voor- en achternaam, zakelijke e-mailadressen, adres, telefoonnummer. En van leveranciers zijn betrokken: zakelijke e-mailadressen, voor- en achternaam, adres, e-mailadres, telefoonnummer.

[26] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[27] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020 – Bijlage 3: Toelichting bij bijlage 2.

Ook blijken er tot 10 C.V.-bestanden van potentiele medewerkers betrokken. Hierin bevonden zich voor- en achternaam, adres, e-mailadres, telefoonnummer en geboortedatum.

In de melding aan de betrokken passagiers (80.000) die Transavia heeft verstuurd meldt Transavia de volgende betrokken gegevens: voornaam, achternaam, geboortedatum, vluchtgegevens, boekingsnummer en de bijgeboekte service zoals bagage, maar ook rolstoelgebruik.[28] Verder geeft Transavia aan dat de betrokken werknemers ook zijn geïnformeerd.[29]

De bijgeboekte services werden beschreven als SSR-code. SSR-code staat voor "*Special Service Request*" code. Transavia gebruikt in hun boekingssysteem een reeks van 4 tekens voor additionele verzoeken, zoals een fiets als bagage. De SSR-code is dan "*BIKE*".[30] Deze codes zijn te vinden op het internet waardoor de betekenis bekend is, mocht dit niet al duidelijk zijn uit de code.[31]

De AP heeft aan Transavia gevraagd welke SSR-codes Transavia gebruikt en in welke aantallen. De door Transavia gebruikte codes geven onder andere aan wanneer een rolstoel benodigd is, of dat een passagier bijvoorbeeld een elektrische rolstoel gebruikt. Codes voor dieetwensen gebruikt Transavia niet aangezien ze geen maaltijden verstrekken tijdens de vluchten.[32]

In de bestanden die zijn gekopieerd naar een externe locatie kwamen codes die rolstoelgebruik indiceren 358 maal voor. Ook kwam een code die blindheid aangeeft vijfmaal voor. Doofheid kwam vier keer voor.[33]

Volgens Transavia waren de passagiersgegevens verzameld in de periode van 21 tot en met 31 januari 2015.[34] De gegevens bevonden zich in een mailbox op "*managed devices van medewerkers*".[35] Dit zijn beheerde apparaten, veelal mobiele apparaten zoals telefoons of laptops. De medewerkers in kwestie waren [VERTROUWELIJK].

2.2.2 Persoonsgegevens waar toegang toe mogelijk was

Hieronder staat een overzicht van de systemen waar de gebruikers [VERTROUWELIJK] en [VERTROUWELIJK] tezamen toegang toe hadden.[36] De titel '*host*' betekent in dit geval de naam van het systeem. De kolom "*Gegevens vanaf ingezien /Geexfiltreerd*" geeft aan of er na het inloggen op het systeem nog andere acties zijn waargenomen. Indien er door Transavia "*nee*" is weergegeven is er alleen ingelogd volgens Transavia.[37]

[28] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.
[29] Zie Dossierstuk 12, Vervolgmelding van 18 februari 2020.
[30] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.
[31] Zie bijvoorbeeld: https://wheelchairtravel.org/air-travel/special-service-request-codes/, of https://guides.developer.iata.org/docs/en/list-of-service-ssrs.
[32] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.
[33] Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020 - Bijlage 5: Overzicht aantallen SSR-codes.
[34] Zie Dossierstuk 13, Persbericht Transavia.
[35] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[36] Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020 – Bijlage 4: Host en Persoonsgegevens.
[37] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.

Datum
23 september 2021

Ons kenmerk
[VERTROUWELIJK]

[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK].	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]

[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]

[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]
[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]	[VERTROUWELIJK]

Uit de bovenstaande tabellen blijkt dat van passagiers de volgende gegevens verwerkt worden: de voor- en achternaam, de geboortedatum, het geslacht, het e-mailadres en telefoonnummer, de vlucht- en boekingsgegevens en de (zakelijke) e-mailcorrespondentie.

Van medewerkers zijn de voor- en achternaam, het geslacht, de geboortedatum, het werknemersnummer, het huisadres, het telefoonnummer, de kwalificaties/training, BSN, de aanwezigheidsadministratie en inloggegevens verwerkt. Verder staat genoemd in het overzicht dat op een systeem verslagen over veiligheidsincidenten aan boord bevonden. Hierin zijn ook mogelijk persoonsgegevens van medewerkers en passagiers betrokken.

In totaal staan voor passagiers tot 25.000.000 betrokkenen genoemd in het aangeleverde overzicht. Voor medewerkers worden tot 3000 betrokkenen genoemd. Dit betekent dat de aanvaller persoonsgegevens heeft ingezien of had kunnen inzien van 25 miljoen mensen.

De mate van activiteit van de aanvaller is door het de externe dienstverlener opgesplitst in de volgende categorieën:[38]

- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]

Op alle genoemde systemen is er sprake van [VERTROUWELIJK].[39] Op [VERTROUWELIJK] systemen is daadwerkelijk bewijs gevonden voor het kopiëren van persoonsgegevens. Systeem [VERTROUWELIJK] is als kritiek aangemerkt door Transavia vanwege de hoeveelheid persoonsgegevens. Op dit systeem was er zowel sprake van [VERTROUWELIJK].

Op het systeem [VERTROUWELIJK] was het bewijs voor de activiteiten van de aanvaller beperkter dan bij andere systemen, omdat er logbestanden ontbraken over de relevante periode van de inbreuk.[40] Verder is het systeem [VERTROUWELIJK] als kritiek aangemerkt vanwege de hoeveelheid persoonsgegevens op dit systeem.[41] Op dit systeem was er sprake van [VERTROUWELIJK].

In de melding aan de AP heeft Transavia aangegeven dat de betrokkenen afkomstig zijn uit meerdere landen, namelijk geheel Europa. De AP heeft Transavia verzocht een overzicht heeft uit welk land de betrokkenen komen. Hierop heeft Transavia geantwoord dat 90% van de klanten uit Nederland komt, gebaseerd op de Point of Sale.[42] Slechts een beperkt aantal persoonsgegevens van zustermaatschappij Transavia France S.A.S. waren op de systemen van Transavia Airlines C.V. aanwezig.[43]

[38] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 19.
[39] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 32.
[40] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 17.
[41] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 4.
[42] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[43] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.

De AP komt tot de conclusie dat Transavia ten tijde van de inbreuk persoonsgegevens verwerkte van ruim 25 miljoen personen. Hiervan zijn persoonsgegevens gelekt van tot 83.000 personen en gezondheidsgegevens van 367 personen.

2.3 Beveiliging ten tijde van de inbreuk

2.3.1 Toegang tot het [VERTROUWELIJK] domein

In het wachtwoordbeleid van Transavia staat aangegeven welke eisen er gelden per gebruiker, per mogelijk risiconiveau.[44] In het wachtwoordbeleid van Transavia staan 3 niveaus vermeldt:

- "*Minimal baseline",* het standaard niveau;
- *"Medium Additions",* additionele maatregelen voor gebruikers met meer bevoegdheden;
- *"Medium and High additions",* extra maatregelen voor bepaalde hoog risico gebruikers.

De gebruikers die gebruikt zijn door de aanvaller hadden volgens Transavia de volgende niveaus:[45]

- [VERTROUWELIJK] had als niveau: **minimal baseline**
- [VERTROUWELIJK] had niveau: **Medium and High security additions**

De externe dienstverlener heeft aangegeven dat de [VERTROUWELIJK] gebruikers "*contained the highest possible privileges*".

Een gebruiker met minimal baseline heeft volgens het wachtwoordbeleid de volgende wachtwoordeisen:[46]

- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]

Voor High security additions zijn de volgende aanvullende eisen van toepassing:[47]

- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]
- [VERTROUWELIJK]

[44] Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020 – Bijlage 1: Personnel & Access Control Standard.
[45] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[46] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020 – Bijlage 1: Personnel & Access Control Standard.
[47] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020 – Bijlage 1: Personnel & Access Control Standard.

Transavia onderscheidt twee typen gebruiker accounts: "*user accounts*" en "*generieke accounts*". De "*user accounts*" betreffen individuele personen. De "*generieke accounts*" bestaan voor meerdere personen of systemen, onder andere voor koppelingen tussen systemen. Inloggen op deze gebruikers vindt veelal automatisch plaats volgens Transavia.[48]

De AP heeft aan Transavia gevraagd waarom de accounts die betrokken waren bij de inbreuk niet voldeden aan de eigen standaarden van Transavia. Transavia geeft in haar antwoord aan dat de focus lag op "*user accounts*" als het gaat om naleving van het wachtwoordenbeleid. Dit zijn in verhouding meer accounts en er werd geacht dat hieruit de meeste risico's zouden voortvloeien. Ook heeft Transavia aangegeven dat deze aanpak de "*awareness*" zou verhogen binnen de organisatie. Vanwege deze focus zouden de tekortkomingen voor de generieke accounts betrokken in de inbreuk niet zijn opgemerkt.[49]

In het wachtwoordbeleid staat verder dat er voor "*remote access*" meerfactorauthenticatie vereist is.[50] Uit het rapport blijkt dat dit niet het geval was voor de gebruikers waarmee de aanvaller toegang heeft kunnen verkrijgen. Zo is toegang geweest tot een Citrix omgeving zonder meerfactorauthenticatie. De externe dienstverlener geeft als een van de aanbevelingen aan Transavia het implementeren van meerfactorauthenticatie voor gebruikers wiens accounts toegankelijk zijn vanaf het internet of in ieder geval voor gebruikers met veel rechten.[51] Citrix zelf adviseert zelf ook om meerfactorauthenticatie voor het gebruik van hun applicatie in te voeren.[52]

De AP heeft aan Transavia gevraagd waarom toegang mogelijk was tot een telewerkomgeving zonder gebruik te maken van meerfactorauthenticatie bij de accounts betrokken in de inbreuk.[53]

Als antwoord heeft Transavia aangegeven dat eerst voor de "*user accounts*" is begonnen met de uitrol van deze maatregelen. De implementatie van deze maatregelen bij de "*user accounts*" duurde langer dan verwacht. Vliegend personeel maakt bij haar werkzaamheden gebruik van applicaties die nodig zijn voor een veilige vlucht. Indien een maatregel zoals meerdere factoren authenticatie vertraging zou veroorzaken, zou dit grote vertragingen bij vluchten kunnen veroorzaken. "*Generieke accounts*" hadden lagere prioriteit bij Transavia. Omdat de implementatie bij het vliegend personeel vertraagd was, was de implementatie bij de "*generieke accounts*" ook vertraagd.[54]

[48] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.
[49] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.
[50] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020 – Bijlage 1: Personnel & Access Control Standard.
[51] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 21.
[52] Zie Dossierstuk 40, Citrix best practices, 9 april 2019.
[53] Dossierstuk 30, Brief AP aan Transavia van 4 september 2020.
[54] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.

De AP heeft aan Transavia gevraagd of periodieke controles plaatsvonden van het beveiligingsbeleid en de feitelijke implementatie hiervan. Transavia heeft hierop aangegeven dat er meerdere periodieke controles plaatsvinden: [55]

- [VERTROUWELIJK][56]
- [VERTROUWELIJK]
- [VERTROUWELIJK]

Bij de [VERTROUWELIJK] controle is ook aangegeven dat voor geprivilegieerde accounts (accounts met veel toegangsrechten) er controle moet plaatsvinden of de wachtwoorden voldoen aan het beleid van Transavia.[57] Transavia heeft als voorbeeld hiervan de resultaten aangeleverd van een [VERTROUWELIJK] controle van 2019, kwartaal 3. De bevindingen gaan over de periode van 12 maanden vóór het onderzoek. Hierin staan positieve en negatieve resultaten aangegeven. Bij meerdere systemen is hier aangegeven dat de wachtwoorden niet voldeden aan het beleid van Transavia.[58]

De AP stelt vast dat de gebruikte wachtwoorden in de aanval niet aan de eisen voldeden van het wachtwoordbeleid van Transavia. Ook was voor deze gebruikers geen meerfactorauthenticatie aanwezig, terwijl deze gebruikers wel toegankelijk waren via het internet of via telewerk software.

2.3.2 Toegang binnen het [VERTROUWELIJK] domein

De aanvaller had tijdens de inbreuk toegang tot vrijwel het hele [VERTROUWELIJK] domein. Transavia heeft meer netwerksegmentatie als vervolgmaatregel doorgevoerd.[59] Volgens het Nationaal Cyber Security Centrum (NCSC) is netwerksegmentatie het "*netwerk opdelen in functionele segmenten*". Met netwerksegmentatie worden alleen de systemen die onderling moeten communiceren samen in aparte segmenten geplaatst. "*Gebruikers krijgen alleen toegang tot de segmenten die zij nodig hebben.*".[60]

De AP heeft aan Transavia gevraagd of de aanvaller bij de systemen waar automatisch toegang toe is verkregen ook andere zaken had kunnen doen zoals gegevens kopiëren, inzien of anderzijds bewerken.[61] Transavia heeft aangegeven dat de aanvaller deze mogelijkheid had.

In de schriftelijke reactie noemt Transavia een aantal beveiligingsmaatregelen die van kracht waren op het moment van de inbreuk: "*Op het moment van de inbreuk had Transavia verschillende maatregelen getroffen in het kader van haar beveiligingsbeleid om de gevolgen van een onbevoegde inlogpoging te voorkomen, waaronder monitoring. Zo werden met het voor Transavia door haar IT-leverancier ingerichte Security Operations Centre de computer- en netwerkactiviteiten van Transavia in de gaten gehouden en gecontroleerd op afwijkende activiteiten. Via dit systeem*

[55] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.
[56] Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020 - Bijlage 6: [VERTROUWELIJK].
[57] Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020 - Bijlage 6: [VERTROUWELIJK].
[58] Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020 - Bijlage 7: Resultaten [VERTROUWELIJK] 2019 – Q3.
[59] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[60] Zie Dossierstuk 41, NCSC, Ransomware, maatregelen voor het voorkomen, beperken en herstellen van een ransomware-aanval, juni 2020.
[61] Dossierstuk 30, Brief AP aan Transavia van 4 september 2020.

ontving Transavia op 21 oktober 2019 de beveiligingsmelding van haar IT-leverancier die duidde op ongeautoriseerde toegang tot het IT-landschap van Transavia."[62]

In het forensisch rapport is aangegeven dat de beheerder logging mogelijkheden had ingericht, waardoor de externe dienstverlener de gebeurtenissen voor een groot gedeelte heeft kunnen reconstrueren. De externe dienstverlener heeft gebruik kunnen maken van de [VERTROUWELIJK][63] omgeving van Transavia.[64]

Uit onderzoek bleek dat het mogelijk was om bepaalde logbestanden te verwijderen. Aangegeven is dat gedurende een week op tenminste [VERTROUWELIJK] systemen logbestanden zijn verwijderd. Ook is beschreven dat bepaalde logging niet bijgehouden werd in de gecentraliseerde omgeving, waaronder van Citrix en van bepaalde kritieke systemen. Een aanbeveling van de externe dienstverlener is dan ook de centrale logging uit te breiden om de integriteit hiervan te bewaken. Ook zou dit leiden tot betere respons op incidenten.[65]

In het forensisch rapport staat verder dat op diverse systemen verouderde besturingssystemen geïnstalleerd waren. Ook staat er dat de geïmplementeerde meerfactorauthenticatie op bepaalde systemen dusdanig was ingeregeld dat een gebruiker zelf een telefoonnummer kon invullen om een tweede factor bericht op te ontvangen. Bepaalde systemen hadden ongecontroleerd toegang tot het internet. Hierdoor heeft de aanvaller kunnen communiceren met externe systemen vanuit het netwerk van Transavia.[66] Tot slot was er onvoldoende netwerk indringer detectie aanwezig was. Hierdoor was er sprake van een beperkt zicht op netwerkactiviteit van de aanvaller.[67]

2.4 Maatregelen na de inbreuk

Nadat Transavia op 21 oktober 2019 erachter is gekomen dat een aanvaller ongeautoriseerde toegang heeft gehad tot haar systemen, heeft Transavia direct door een externe dienstverlener een forensische analyse laten uitvoeren. Na de vaststelling van de inbreuk heeft Transavia verschillende maatregelen genomen.

Transavia heeft onder andere voor alle eindgebruikers en apparaten tweefactor-authenticatie ingevoerd. Daarnaast zijn de wachtwoorden van alle gebruikers- en generieke accounts gereset en zijn wachtwoordvereisten technisch doorgevoerd. Tot slot heeft Transavia haar netwerk opgedeeld in meerdere segmenten.[68]

[62] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[63] [VERTROUWELIJK] maakt het mogelijk om gegevens uit een grote hoeveelheid verschillende bronnen (geautomatiseerd) te analyseren en signaleringen te ontvangen hierop. Een gecentraliseerde omgeving waarbij een systeem logging uit verschillende bronnen verzamelt, analyseert en rapporteert wordt ook wel een Security Information and Event Management (SIEM) genoemd. Zie ook: Dossierstuk 42, NCSC, Handreiking voor implementatie van detectie oplossingen, oktober 2015.
[64] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 4.
[65] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 23 en 29.
[66] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 27 en 28.
[67] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 29.
[68] Schriftelijke zienswijze Transavia, 28 juni 2021, pagina 7 en 8.

2.5 Zienswijze Transavia op de vastgestelde feiten en reactie AP

Transavia heeft in haar zienswijze enkele feiten genuanceerd en de AP gevraagd om deze punten aan te passen.[69] Voor zover relevant voor dit besluit benoemt de AP deze zienswijze in het kort, voorzien van een reactie van de AP.

Transavia wil allereerst benadrukken dat de accounts [VERTROUWELIJK] alleen tezamen (en niet ieder voor zich) toegang gaven tot een groot deel van het computernetwerk van Transavia. En dat de overzichten zien op de gegevens waartoe de accounts tezamen toegang hadden. De AP betwist dit feit niet. In het rapport van de AP is beschreven dat via toegang tot het eerste account er toegang is verkregen tot het tweede account. Niettemin heeft de AP in het besluit een verdere nuancering hierover opgenomen.

Ten tweede benoemt Transavia dat de geëxfiltreerde gegevens niet met name uit contactgegevens bestonden. Dit in tegenstelling tot de bestanden die door aanvaller alleen zijn ingezien of had kunnen inzien. Het bestand met historische passagiersgegevens bevatte geen contactgegevens, alleen voor- en achternaam, geboortedatum, vluchtinformatie en SSR-code. De andere geëxfiltreerde bestanden bevatten wel zakelijke contactgegevens van werknemers en zakelijke contacten, maar verhoudingsgewijs betreffen dit volgens Transavia minder gegevens. De AP beaamt dit standpunt van Transavia en heeft dit aangepast.

Tot slot geeft Transavia aan dat uit een passage van het rapport opgesteld door de externe dienstverlener niet zozeer af te lezen is dat systemen *onnodig* toegang hadden tot het internet, maar dat deze systemen door het ontbreken van host based firewalls ongecontroleerde of ongewaarborgde toegang hadden tot het internet. Als reactie hierop heeft de AP het woord ‘onnodig’ vervangen door ‘ongecontroleerde’.

[69] Schriftelijke zienswijze Transavia, 28 juni 2021.

3. Beoordeling

3.1 Persoonsgegevens en grensoverschrijdende verwerking

Transavia verwerkt gegevens van passagiers, werknemers en leveranciers. Gegevens zoals namen en geboortedatums zijn gegevens waarmee Transavia natuurlijke personen kan identificeren. Dit kan zowel direct of indirect door het combineren van gegevens. Omdat Transavia gegevens verwerkt waarmee een persoon direct of indirect mee kan worden geïdentificeerd, verwerkt Transavia persoonsgegevens zoals genoemd in artikel 4, onderdeel 1, van de AVG.

Verder verwerkt Transavia persoonsgegevens met betrekking tot rolstoelgebruik, doofheid en blindheid. Omdat deze informatie, samen met andere gekoppelde informatie, iets zegt over de gezondheid van een klant van Transavia, verwerkt Transavia ook bijzondere categorieën persoonsgegevens zoals aangegeven in artikel 9, lid 1, van de AVG.

Transavia biedt diensten aan in meerdere Europese landen. Ook wordt er gevlogen naar en uit meerdere Europese landen.[70] De passagiersgegevens van Transavia betreffen hierdoor gegevens van betrokkenen uit meerdere Europese landen. Transavia heeft aangegeven dat persoonsgegevens die Transavia verwerkt voor 90% waarschijnlijk afkomstig zijn uit Nederland, gebaseerd op "*point of sale*".[71] Gezien het aantal persoonsgegevens dat Transavia verwerkt van Europeanen, acht de AP 10% nog steeds een substantieel aantal.

Omdat bij de verwerkingen van Transavia vanuit tenminste één vestiging betrokkenen uit meerdere lidstaten wezenlijke gevolgen zullen ondervinden, of waarschijnlijk zullen ondervinden, is er volgens de AP sprake van een grensoverschrijdende verwerking zoals bedoeld in artikel 4, onderdeel 23, van de AVG.

3.2 Verwerkingsverantwoordelijke

In het privacy beleid van Transavia Airlines C.V. is aangegeven dat Transavia verantwoordelijk is voor de persoonsgegevens die Transavia verwerkt. Verder heeft Transavia aangegeven dat de Franse maatschappij zelf verantwoordelijk is voor de gegevens die deze tak verzamelt.[72]

Transavia Airlines C.V. heeft afspraken met zustermaatschappij Transavia France S.A.S gemaakt indien Transavia France S.A.S gebruik maakt van de systemen van Transavia Airlines C.V. door middel van een Service Level Agreement. In deze afspraken staat dat het beheer van de ICT systemen de verantwoordelijkheid is van Transavia Airlines C.V. [73]

[70] Zie Dossierstuk 44, Afdruk website bedrijfsprofiel en www.transavia.com.
[71] Zie Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020.
[72] Zie Dossierstuk 39, Privacy beleid Transavia.
[73] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020 en bijlage 2: Fragment uit SLA Transavia Airlines C.V. – Transavia France S.A.S en bijlage 3: Mail Transavia Airlines C.V. aan Transavia France S.A.S.

Wat betreft de werknemersgegevens heeft Transavia aangegeven dat deze gegevens gescheiden worden verwerkt.[74] Dit wil zeggen dat zowel de Franse als Nederlandse organisatie zelfstandig verantwoordelijk zijn voor deze gegevens van hun eigen medewerkers. Transavia heeft documentatie aangeleverd waaruit blijkt dat ook werknemersgegevens zich op systemen van Transavia Airlines C.V. bevinden. [75]

Verder heeft Transavia aangegeven dat ten tijde van de inbreuk op slechts een beperkt aantal systemen persoonsgegevens aanwezig waren van Transavia France S.A.S. [76]

Transavia Airlines C.V. was daarnaast de opdrachtgever voor het onderzoek door de externe dienstverlener. Transavia Airlines C.V. is ook de partij die geïnformeerd is door de beheerder en een melding heeft gedaan van de inbreuk bij de AP en de betrokkenen.[77]

Gelet op het bovenstaande stelt Transavia Airlines C.V. het doel en middelen vast van (een groot gedeelte) van de persoonsgegevens op de systemen zoals eerder vernoemd in hoofdstuk 2. De AP stelt vast dat Transavia Airlines C.V. de verwerkingsverantwoordelijke is zoals bedoeld in artikel 4, onderdeel 7 van de AVG.

Het hoofdkantoor van Transavia Airlines C.V. is verder gevestigd in Schiphol, Nederland.[78] Gelet op het feit dat hierboven is vastgesteld dat Transavia Airlines C.V. als verwerkingsverantwoordelijke kan worden aangemerkt, is de AP de leidende toezichthouder. Volgens artikel 56 van de AVG heeft de AP in het Europese samenwerkingssysteem IMI met de andere toezichthouders overlegd over het feit dat de AP zichzelf als leidende toezichthouder ziet. Uit deze procedure is geen tegenspraak hierop gekomen van andere Europese toezichthouders.

3.3 Passende beveiligingsmaatregelen

3.3.1 Inleiding

In artikel 32 van de AVG zijn de eisen rondom de beveiliging van de verwerking van persoonsgegevens opgenomen. De verwerkingsverantwoordelijke dient passende technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bij het bepalen van passende maatregelen dient rekening gehouden te worden met het risico voor de rechten en vrijheden van personen.

De AP toetst in het navolgende of de technische maatregelen bij Transavia met betrekking tot de toegang tot persoonsgegevens passend waren als bedoeld in artikel 32 van de AVG.

[74] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.
[75] Dossierstuk 25, Antwoorden van Transavia, datum 26 mei 2020 – Bijlage 3: Toelichting bij bijlage 2.
[76] Zie Dossierstuk 38, Antwoorden van Transavia datum 24 september 2020.
[77] Zie Dossierstuk 11, rapport van 5 december 2019, pagina 4 en dossierstuk 1 en 13.
[78] Zie Dossierstuk 26, Inschrijving Handelsregister Transavia Airlines C.V.

3.3.2 Beoordeling

Om te bepalen wat passend is dient er een afweging plaats te vinden tussen de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. En een op risico afgestemd beveiligingsniveau omvat onder meer het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen (artikel 32, lid 1, sub b van de AVG).

Stand van de techniek en uitvoeringskosten
Zoals vastgesteld in hoofdstuk 2 gebruikte de aanvaller een "*password spray*" of "*credential stuffing*" aanval waarbij een hacker veelgebruikte of eerder gelekte wachtwoorden toepast. De maatregelen die hiertegen genomen kunnen worden hangen onder meer samen met het type applicatie en de mogelijkheden. In deze inbreuk bleek echter de oorzaak van de inbreuk een eenvoudig en veelgebruikt wachtwoord bij twee gebruikers die makkelijk (geautomatiseerd) te raden was. De sterkte en het niveau van het wachtwoord was niet conform het eigen authenticatiebeleid van Transavia.

Vaststaat dat Transavia een beleid heeft voor de authenticatie van gebruikers. Ook staat vast dat Transavia periodieke controles uitvoert en voortdurend werkt aan haar eigen beveiligingsbeleid. Uit de door Transavia aangeleverde periodieke beveiligingscontroles blijkt echter dat bij veel applicaties er niet voldaan werd aan het wachtwoordbeleid van Transavia zelf.

Transavia heeft aangegeven dat de generieke accounts die gebruikt zijn gedurende de inbreuk niet de focus hadden tijdens interne controles. Zo is niet gecontroleerd of de wachtwoorden van generieke accounts volgens het eigen beleid werden gebruikt. Volgens Transavia lag het risico bij andere typen accounts, namelijk de gebruikersaccounts gekoppeld aan individuele gebruikers. Hierdoor zijn de slechte wachtwoorden niet tijdig opgemerkt volgens Transavia. Verder is aangegeven dat meerfactorauthenticatie implementeren voor "*generieke accounts*" nog niet was gerealiseerd op het moment van de inbreuk, omdat de implementatie bij andere gebruikers vertraging had opgelopen.

Na de eerste succesvolle authenticatie werd gebruik gemaakt van een Citrix omgeving. Deze omgeving is vervolgens door de aanvaller gebruikt om verdere toegang te verkrijgen tot de systemen van Transavia. Voor dit soort omgevingen wordt aangeraden om meerfactorauthenticatie te gebruiken om toegang te beperken. Zoals eerder vermeld is dit een veelvoorkomende maatregel die ook ten tijde van de inbreuk geadviseerd werd door de aanbieder van de telewerksoftware Citrix.

Nadat de aanvaller zich verdere toegang had verschaft, had hij/zij veel vrijheden op de systemen van Transavia. Uiteindelijk heeft dit geresulteerd in het kopiëren van persoonsgegevens uit mailboxen van medewerkers. Dit had voorkomen kunnen worden door het netwerk op te delen in meerdere segmenten. Verder kunnen de rechten van gebruikers aangepast worden, om te bepalen of het nodig is dat deze gebruikers deze rechten hebben (autorisaties). Transavia heeft deze maatregel na de inbreuk geïmplementeerd.

Het bleek verder mogelijk om op systemen, die als kritiek zijn aangemerkt door Transavia, logbestanden te verwijderen. Hierdoor was er na de inbreuk geen volledig beeld van wat er gebeurd was op deze systemen.

Veelgebruikte standaarden op het gebied van informatiebeveiliging die geldig waren ten tijde van de inbreuk geven op het gebied van wachtwoordbeheer, netwerksegmentatie en de rechten van gebruikers verschillende aanbevelingen. Zo wordt als beheersmaatregel genoemd het waarborgen van sterke wachtwoorden. Ook moeten groepen van informatiesystemen in netwerken worden gescheiden. Verder wordt aangegeven dat toegangsrechten moeten worden beperkt en gecontroleerd en dient toegang tot informatie te worden beperkt. [79]

De maatregelen die Transavia had kunnen nemen ten tijde van de inbreuk, waren reeds een norm volgens Transavia zelf, volgens leveranciers en volgens internationale standaarden. Verder bleek dat er bepaalde maatregelen wel al deels waren geïmplementeerd door Transavia.

Op grond van bovenstaande is de AP van mening dat, gelet op de stand van de techniek ten tijde van de inbreuk, het zeker mogelijk was om beveiligingsmaatregelen te implementeren voor het risico dat zich heeft gerealiseerd in de inbreuk. De invoering van bovengenoemde essentiële voorzorgsmaatregelen zouden het mogelijk hebben gemaakt om de vertrouwelijkheid van de verwerkte persoonsgegevens overeenkomstig artikel 32, lid 1, sub b van de AVG te waarborgen en het risico van het optreden van het datalek substantieel te verminderen.

Uit de door Transavia aangeleverde informatie blijkt verder dat er na de inbreuk een veelvoud aan maatregelen zijn genomen waaronder het aanpassen van wachtwoorden, het implementeren van netwerksegmentatie en het aanpassen van gebruikersrechten. De AP acht de uitvoeringskosten voor deze beveiligingsmaatregelen niet dusdanig hoog dat deze maatregelen niet eerder geïmplementeerd konden worden.

De aard, de omvang, de context en de verwerkingsdoeleinden
Naarmate de gegevens bijvoorbeeld op grote schaal worden verwerkt en een gevoeliger karakter hebben, worden zwaardere eisen gesteld aan de beveiliging van de gegevens.

De AP heeft vastgesteld dat Transavia een grote hoeveelheid persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens zoals gezondheidsgegevens. De aanvaller had toegang tot systemen waar zich gegevens bevinden van ongeveer 25 miljoen passagiers. Gezien deze grootschalige verwerking van persoonsgegevens acht de AP de beveiliging van Transavia ten tijde van de inbreuk niet adequaat.

Waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen
In de inbreuk is er sprake geweest van ongeoorloofde toegang en verstrekking van persoonsgegevens. Verder had de aanvaller niet alleen toegang kunnen hebben tot veel meer persoonsgegevens, het was ook mogelijk om deze gegevens te kopiëren of anderzijds te verwerken. De gegevens die Transavia verwerkt, zoals contactgegevens, kunnen in handen van een kwaadwillende derde misbruikt worden voor doeleinden die kunnen leiden tot materiele of immateriële schade.[80] Transavia verwerkt daarnaast ook

[79] Zie dossierstuk 43: NEN-norm_ISO_27001_2017_nl, pagina 23, 24 en 29.
[80] Zo kunnen contactgegevens gebruikt worden door een kwaadwillende derde voor phishing. Phishing is gericht op het verkrijgen van (gevoelige) informatie, om hiermee fraude te plegen. Zie ook: https://www.ncsc.nl/onderwerpen/phishing.

bijzondere persoonsgegevens van passagiers en BSN-nummers van werknemers. Een inbreuk op de vertrouwelijkheid hiervan kan leiden tot immateriële schade, zoals discriminatie of fraude.[81]

Passende technische maatregelen
Gelet op bovenstaande is de AP van oordeel dat de technische maatregelen niet 'passend' waren ten tijde van de inbreuk, zoals bedoeld in artikel 32 van de AVG. Gezien de hoeveelheid en het soort persoonsgegevens dat Transavia verwerkt moet een hoog niveau van maatregelen worden genomen. Een inbreuk op de vertrouwelijkheid van deze gegevens kan namelijk voor veel personen materiele of immateriële schade tot gevolg hebben.

De maatregelen die Transavia had kunnen nemen waren mogelijk en passend gezien de stand van de techniek en de uitvoeringskosten. Het gebrek aan deze maatregelen, op meerdere niveaus, heeft geleid tot een (gerealiseerd) risico voor de rechten en vrijheden van betrokkenen.

3.3.3 Zienswijze Transavia en reactie AP

De AP geeft hieronder de zienswijze van Transavia op de beoordeling van de AP in het kort weer, voorzien van een reactie van de AP.

Zienswijze Transavia
Transavia geeft in haar zienswijze aan dat zij een doorlopende verbeteringsproces cyclisch heeft ingebed in haar organisatie volgens de in de sector algemeen gehanteerde normering en Plan-Do-Check-Act cyclus (PDCA). Tegen deze achtergrond heeft Transavia beleid voor authenticatie van gebruikers (het 'Authenticatiebeleid') in december 2017 vastgesteld met een beleidshorizon van drie jaar (fase 'Plan'). Transavia beseft dat de wachtwoorden van de gecompromitteerde accounts in 2019 niet voldeden aan het eigen Authenticatiebeleid. Hoewel het Authenticatiebeleid volgens Transavia zelf passend was, zoals bedoeld in artikel 32 AVG, was de implementatie van dat beleid niet volledig. De wachtwoorden van de gecompromitteerde accounts voldeden niet aan het eigen beleid en waren in die zin niet passend voor het beoogde niveau van beveiliging.

Transavia wil echter het beeld van de AP in het onderzoeksrapport rondom multi-factor authenticatie nuanceren. Op basis van de destijds beschikbare informatie verwachtte Transavia dat de kans op een succesvolle 'password spray' aanval of 'credential stuffing attack' groter was bij gebruikersaccounts dan bij generieke accounts. Gegevens over gebruikersaccounts zijn over het algemeen veel makkelijker te vinden op internet (denk aan naam persoon in combinatie met de organisatie, gegevens op Linkedin), dan gegevens over generieke accounts die niet zijn gekoppeld aan een persoon. Daarnaast speelde bij deze afweging voor Transavia een belangrijke rol dat het aantal gebruikersaccounts in verhouding vele malen groter was dan het aantal generieke accounts. Transavia wil benadrukken dat zij de keuze om prioriteit te geven aan gebruikersaccounts zorgvuldig heeft genomen, rekening houdend met de op dat moment

[81] Zie ook: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken#wanneer-levert-een-datalek-een-hoog-risico-op-7331.

voorzienbare risico's. Tot slot wil Transavia opmerken dat zij, voor wat betreft de invoering van multi-factor authenticatie tussen 2017 en 2019, in de pas liep met de rest van de industrie.

Reactie AP
De AP heeft geconstateerd dat de beveiligingsmaatregelen op meerdere niveaus onvoldoende passend waren. De combinatie van zwakke wachtwoorden en het ontbreken van een tweefactor-authenticatie maakte het volgens de AP voorzienbaar dat er een groot risico bestond op ongeoorloofde toegang tot de persoonsgegevens van Transavia. Tweefactor-authenticatie is al jarenlang een gangbare beveiligingsmaatregel en vrij eenvoudig om te implementeren. De AP ziet op grond van de nuancering van Transavia over meerfactorauthenticatie geen aanleiding om de beoordeling hierover aan te passen.

3.4 Conclusie

De AP komt tot de conclusie dat Transavia ten tijde van de inbreuk geen passende maatregelen getroffen heeft om een op het risico afgestemd beveiligingsniveau te waarborgen. Hierdoor heeft Transavia in strijd gehandeld met artikel 32, eerste en tweede lid, van de AVG.

4. Boete

4.1 Inleiding

Transavia heeft in strijd gehandeld met artikel 32, eerste en tweede lid, van de AVG. De AP maakt voor de vastgestelde overtreding gebruik van haar bevoegdheid om aan Transavia een boete op te leggen. Gezien de ernst van de overtreding en de mate waarin deze aan Transavia kan worden verweten, acht de AP de oplegging van een boete gepast. De AP motiveert dit in het navolgende.

4.2 Boetebeleidsregels Autoriteit Persoonsgegevens 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 Transavia in geval van een overtreding van artikel 32 van de AVG een bestuurlijke boete op te leggen tot € 10.000.000 of, voor een onderneming, 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.[82] In de Boetebeleidsregels is gekozen voor een categorie-indeling en bandbreedte systematiek. Overtreding van artikel 32 van de AVG is ingedeeld in categorie II. Categorie II heeft een boetebandbreedte tussen € 120.000 en € 500.000 en een basisboete van € 310.000.

4.3 Boetehoogte

De hoogte van de boete stemt de AP af op de factoren die zijn genoemd in artikel 7 van de Boetebeleidsregels, door het basisbedrag te verlagen of verhogen. Het gaat om een beoordeling van de ernst van de overtreding in het specifieke geval, de mate waarin de overtreding aan de overtreder kan worden verweten en, indien daar aanleiding toe bestaat, andere omstandigheden.

4.3.1 Ernst van de overtreding

De AP is tot de conclusie gekomen dat Transavia geen passend beveiligingsniveau heeft gehanteerd voor de verwerking van persoonsgegevens in haar netwerk. Transavia verwerkt vele soorten persoonsgegeven, zoals contactgegevens van passagiers en het BSN, de aanwezigheidsadministratie en inloggegevens van haar medewerkers. Verder verwerkt Transavia ook gezondheidsgegevens, zoals het rolstoelgebruik, doofheid en blindheid van passagiers.

Daarnaast is van belang dat Transavia ten tijde van de inbreuk persoonsgegevens verwerkte van ruim 25 miljoen personen. Transavia heeft destijds de persoonsgegevens van deze grote groep betrokkenen

[82] Stcrt. 2019, 14586, 14 maart 2019.

onvoldoende beveiligd. Deze enorme groep burgers hebben onnodig extra risico gelopen op onder andere onbevoegde toegang tot hun persoonsgegevens. Een risico wat overigens is gerealiseerd door de inbreuk uit 2019 waarbij persoonsgegevens van tot 83.000 personen zijn gelekt en gezondheidsgegevens van 367 personen.

Vanwege het feit dat bij deze overtreding de gegevensverwerking omvangrijk is, het een groot aantal betrokkenen betreft en er ook bijzondere persoonsgegevens werden verwerkt kwalificeert de AP deze inbreuk op de AVG als zeer ernstig.

Gelet op het bovenstaande ziet de AP, op grond van de mate van ernst van de overtreding, aanleiding om aan Transavia een boete op te leggen en het (basis)bedrag van de boete te verhogen naar € 400.000.

4.3.2 Verwijtbaarheid, nalatigheid en schadebeperkende maatregelen

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. Nu het hier gaat om een overtreding, is voor het opleggen van een bestuurlijke boete conform vaste rechtspraak niet vereist dat wordt aangetoond dat sprake is van opzet en mag de AP verwijtbaarheid veronderstellen als het daderschap vaststaat. Daarnaast houdt de AP ook rekening met de nalatige aard van de inbreuk en de schadebeperkende maatregelen door Transavia.

Transavia is op grond van artikel 32 van de AVG verplicht om beveiligingsmaatregelen in te voeren die passend zijn voor de aard en omvang van de verwerkingen die Transavia uitvoert. Gelet op de (gevoelige) aard en de grote omvang van de verwerking is de AP van oordeel dat Transavia in elk geval bijzonder nalatig is geweest in het voldoende treffen van dergelijke maatregelen. Van Transavia mag worden verwacht dat zij zich van de voor haar geldende normen vergewist en daar naar handelt. De AP acht dit verwijtbaar.

Daarnaast heeft de AP vastgesteld dat uit de door Transavia aangeleverde periodieke beveiligingscontroles bleek dat bij veel applicaties er niet voldaan werd aan het eigen wachtwoordbeleid van Transavia.
De AP acht het zeer nalatig dat Transavia na deze controles niet meteen in actie is gekomen om zo een passend beveiligingsniveau te waarborgen. Aan de andere kant heeft Transavia na kennisname van het datalek direct vele maatregelen genomen om persoonsgegevens passender te beschermen en om te voorkomen dat de aanvaller zich nog langer in de systemen van Transavia kon begeven. Bovendien heeft Transavia aangegeven dat zij ook in het algemeen meerdere maatregelen heeft genomen om het beveiligingsniveau in het bedrijf te verhogen.

Gelet op de bovenstaande afweging ziet de AP daarom aanleiding om het boetebedrag op grond van de nalatige aard van de inbreuk te verhogen met € 25.000. Maar ook om het boetebedrag op grond van de genomen schadebeperkende maatregelen weer te verlagen met € 25.000.

4.3.3 Overige omstandigheden

Transavia stelt in haar zienswijze dat betrokkenen met aan zekerheid grenzende waarschijnlijkheid geen nadelige gevolgen hebben ondervonden van het datalek. De gelekte gegevens van passagiers bevatte geen contactgegevens en waren niet of beperkt gevoelig. Transavia heeft de afgelopen anderhalf jaar geen melding gehad over misbruik van de gegevens. Verder heeft Transavia het datalek tijdig bij de AP gemeld en de betrokkenen geïnformeerd. Tot slot heeft Transavia zo goed mogelijk meegewerkt aan het onderzoek van de AP en geen winsten gemaakt of verliezen gemeden met de inbreuk.

De AP is van oordeel dat de medewerking van Transavia niet verder is gegaan dan haar wettelijke plicht om te voldoen aan artikel 31 van de AVG. Transavia heeft daarmee niet op bijzondere wijze samengewerkt met de AP. Ook de omstandigheid dat Transavia slechts voldoet aan haar wettelijke meldplicht aan de AP en betrokkenen, kan gezien de ernst van deze overtreding de nakoming van deze verplichting niet als een verlichtende of verzachtende factor worden beschouwd. Tot slot merkt de AP op dat het recht van bescherming van persoonsgegevens van verschillende betrokkenen wel degelijk geschaad is, doordat bijvoorbeeld gezondheidsgegevens van passagiers en contactgegevens van werknemers in handen zijn gekomen van een kwaadwillende derde partij. Deze betrokkenen zijn verhinderd in het behouden van de regie van hun persoonsgegevens.

Deze zienswijze geeft de AP gelet op de ernst van de overtredingen en de mate van verwijtbaarheid geen aanleiding om af te zien van boeteoplegging dan wel de boete op de door Transavia genoemde gronden te matigen.

4.3.4 Evenredigheid

Tot slot beoordeelt de AP ingevolge artikelen 3:4 en 5:46 van de Awb 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.

De AP is van oordeel dat (de hoogte van) de boete evenredig is.[83] De AP heeft in dit oordeel de ernst van de overtreding, de mate waarin deze aan Transavia kan worden verweten, de schadebeperkende maatregelen en overige omstandigheden meegewogen. Vanwege de grote omvang van de gegevensverwerking, het feit dat het een groot aantal betrokkenen betreft en er ook bijzondere persoonsgegevens werden verwerkt kwalificeert de AP deze inbreuk op de AVG als zeer ernstig.

Gezien alle omstandigheden van dit geval ziet de AP geen aanleiding het bedrag van de boete op grond van de evenredigheid en de in de Boetebeleidsregels genoemde omstandigheden, voor zover van toepassing in het voorliggende geval, nog verder te verhogen of te verlagen.

4.4 Conclusie

De AP stelt het totale boetebedrag vast op € 400.000.

[83] Zie voor de motivering paragraaf 4.3.1 en 4.3.2.

Datum
23 september 2021

Ons kenmerk
[VERTROUWELIJK]

5. Dictum

De AP legt aan Transavia Airlines C.V. wegens overtreding van artikel 32, eerste en tweede lid, van de AVG een bestuurlijke boete op ten bedrage van:
€ 400.000 (zegge vierhonderdduizend euro).[84]

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

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. Het indienen van een bezwaarschrift schort de werking van dit besluit op. Voor het indienen van digitaal bezwaar, zie www.autoriteitpersoonsgegevens.nl, onder het kopje 'Bezwaar maken', 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); u kunt ook een kopie van dit besluit bijvoegen
- De reden(en) waarom u het niet eens bent met dit besluit
- Uw handtekening

Zie voor meer informatie: https://autoriteitpersoonsgegevens.nl/nl/bezwaar-maken

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