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
[VERTROUWELIJK]

Datum
6 november 2018

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Besluit tot het opleggen van een bestuurlijke boete

Geachte heren [VERTROUWELIJK],

De Autoriteit Persoonsgegevens (AP) heeft besloten aan uw cliënten Uber B.V. (UBV) en Uber Technologies, Inc. (UTI) gezamenlijk een bestuurlijke boete van **€ 600.000** op te leggen, omdat UBV en UTI, als (gezamenlijk) verantwoordelijke op 15 november 2016, althans in elk geval binnen uiterlijk 72 uur nadat UTI op 14 november 2016 in kennis is gesteld van het datalek hebben nagelaten de AP en betrokkenen in kennis te stellen van het datalek.

De melding aan de AP heeft eerst plaatsgevonden op 21 november 2017. Op diezelfde dag heeft Uber een nieuwsbericht over het datalek op haar website gepubliceerd. Daarmee zijn de AP en betrokkenen niet onverwijld van het datalek in kennis gesteld. Dit is een overtreding van artikel 34a, eerste en tweede lid, van de Wet bescherming persoonsgegevens (Wbp), zoals dat destijds gold.

Hierna wordt het besluit nader toegelicht. In paragraaf 1 staat de weergave van de feiten die ten grondslag liggen aan het besluit. Paragraaf 2 beschrijft het wettelijk kader. In paragraaf 3 beoordeelt de AP haar bevoegdheid, de verantwoordelijkheid voor de gegevensverwerking, de overtredingen en de ernstig verwijtbare nalatigheid. In paragraaf 4 wordt de hoogte van de bestuurlijke boete uitgewerkt. Paragraaf 5 bevat het dictum en de rechtsmiddelenclausule.

Datum
6 november 2018

Ons kenmerk
[VERTROUWELIJK]

1. Feiten en procesverloop

1.1 Betrokken rechtspersonen

Uber B.V.
UBV is een aan de Mr. Treublaan 7, (1097 DP) te Amsterdam statutair gevestigde besloten vennootschap. UBV is opgericht op 24 oktober 2012 en is ingeschreven in het register van de Kamer van Koophandel onder nummer 56317441. UBV is een indirecte volle dochteronderneming van UTI.

Uber Technologies, Inc
UTI is gevestigd te 1455 Market Street, San Francisco, Verenigde Staten. UTI is de uiteindelijke moederonderneming van een groep van tientallen ondernemingen, waaronder ook UBV.

UTI en UBV worden hierna gezamenlijk aangeduid als 'Uber' of als 'Uber-concern'.

1.2 Procesverloop

Op 21 november 2017 heeft UBV melding[1] gedaan van een datalek aan de AP.

Naar aanleiding van die melding is de AP op grond van artikel 60, eerste lid, van de Wbp een ambtshalve onderzoek gestart. In dat kader is op 23 november 2017 een eerste schriftelijk informatieverzoek verstuurd aan UBV. Daarna zijn nog diverse informatieverzoeken gevolgd. Hieraan heeft Uber gevolg gegeven.

De resultaten van het onderzoek naar de melding van voormeld datalek zijn opgenomen in het rapport dat op 1 juni 2018 door de directeur Beleid, Internationaal, Strategie en Communicatie is vastgesteld.[2]

Op 15 juni 2018 heef de AP aan Uber een voornemen gestuurd tot het opleggen van een bestuurlijke boete wegens overtreding van artikel 34a, eerste lid en tweede lid, van de Wbp.

Op 3 juli 2018 heeft Uber schriftelijk haar zienswijze gegeven op het voornemen tot het opleggen van een bestuurlijke boete en het daarvoor opgestelde rapport.

Op 11 juli 2018 heeft ten kantore van de AP een hoorzitting plaatsgevonden waarbij Uber ook mondeling haar zienswijze heeft toegelicht.

Op 14 september 2018 heeft de AP het verslag van de hoorzitting aan Uber toegestuurd. Bij brief van 27 september 2018 heeft Uber haar opmerkingen op het verslag aan de AP kenbaar gemaakt.

Bij brief van 22 oktober 2018 heeft de gemachtigde van Uber aan de AP een nader stuk toegezonden.

[1] Kenmerk [VERTROUWELIJK]
[2] Onderzoeksrapport [VERTROUWELIJK]

1.3 Dienstverlening Uber

Het Uber-concern biedt een dienst aan die het voor gebruikers van die dienst mogelijk maakt om taxiritten te bestellen via onder meer een applicatie (de Uber app). Gebruikers van de Uber app die een taxirit willen bestellen (riders) worden gekoppeld aan chauffeurs (drivers) die via een andere applicatie van het Uber-concern klanten kunnen aannemen (de Uber Driver app). Uber drivers gebruiken hun eigen auto voor het aanbieden van taxiritten, zijn niet in dienst van Uber en kunnen de vraag naar taxiritten van Uber riders aanvaarden of weigeren.

Om gebruik te maken van de Uber apps, zowel als rider of als driver, is het noodzakelijk om een account aan te maken. Hiervoor is het verplicht om voor- en achternaam, telefoonnummer en e-mailadres op te geven. Het doel van de verwerking van deze gegevens is onder meer het hij elkaar brengen van vraag en aanbod naar/van taxiritten en de verwerking van betalingen voor die taxiritten.

1.4 Bewerkersovereenkomst

UBV en UTI hebben op 31 maart 2016 een *'Data Processing Agreement'* (bewerkersovereenkomst) gesloten. Daarin zijn UBV en UTI overeengekomen dat UBV verantwoordelijke is voor de verwerking van persoonsgegevens die zij verzamelt en verwerkt van betrokkenen buiten de Verenigde Staten van Amerika (Verenigde Staten) en dat UTI ten behoeve van UBV die gegevens als bewerker verwerkt.

1.5 Opslag van (persoons)gegevens in de Verenigde Staten

De gegevens van chauffeurs en gebruikers van de Uber-app buiten de Verenigde Staten worden doorgestuurd vanuit Nederland naar de Verenigde Staten. Daar worden zij opgeslagen op servers van UTI in de Verenigde Staten. Gebleken is voorts dat UTI een bewerkersovereenkomst voor het gebruik van data-opslagcapaciteit/servers (AWS S3) is aangegaan met Amazon. Het doel van die opslag is het maken van back-ups van die (persoons)gegevens.

1.6 Datalek en melding aan AP

Op 14 november 2016 is UTI op de hoogte gesteld van een kwetsbaarheid in haar gegevensbeveiliging. Op die datum ontving de toenmalige [VERTROUWELIJK] van UTI een e-mailbericht van een persoon die de [VERTROUWELIJK] informeerde dat hij en zijn team (melder/melders) een grote kwetsbaarheid in de gegevensbeveiliging van het Uber-concern had ontdekt.

De melder heeft in de periode van 13 oktober 2016 tot 15 november 2016 toegang gehad tot AWS S3 opslag van het Uber-concern door middel van inloggegevens die waren opgeslagen in een private GitHub repository van het Uber-concern. Op de servers van Amazon stonden 'rider' (klant-) en 'driver'-(chauffeur)gegevens opgeslagen. Het gaat daarbij om de volgende persoonsgegevens:

1 UserID;
2 DriverID;
3 First and Last name;
4 E-mail address;
5 Mobile number;

6 Last confirmed mobile number;
7 Nickname;
8 Driver's license number;
9 Receipt e-mail;
10 Token;
11 Mobile token;
12 E-mail token;
13 [VERTROUWELIJK];
14 [VERTROUWELIJK];
15 Location of signup (lattitude/longtitude);
16 Signup "shape";
17 Location;
18 Inviter ID;
19 InviterUUID;
20 Recent fare splitter ID;
21 Meta veld;
22 Notes;
23 Driver payment statements;
24 Licence plate numbers;
25 NYC UC numbers;
26 Userrating;
27 Driver rating;
28 Professionalism score;
29 City knowledge score;
30 Banned;
31 Fraud score.

Op 15 november 2016 heeft UTI het datalek verholpen.

Het datalek was aanleiding voor UTI om [VERTROUWELIJK], een forensisch expert, in te schakelen. Het verzoek daartoe is op 18 oktober 2017 gedaan. [VERTROUWELIJK] heeft onderzocht in hoeverre de melders toegang hadden tot gegevens van het Uber-concern die destijd op Amazon servers waren opgeslagen. [VERTROUWELIJK]heeft haar bevindingen vastgelegd in een rapport.[3] Geconstateerd is dat bij het datalek 57.383.315 Uber gebruikers waren betrokken, waarvan 25.606.182 Amerikaanse - en 31.777.133 niet-Amerikaanse. Uit de informatie van UBV blijkt dat ongeveer 174.000 Nederlandse Uber-gebruikers zijn getroffen door het datalek. Uit het door [VERTROUWELIJK]uitgevoerde onderzoek blijkt dat er bij het datalek 31 soorten persoonsgegevens betrokken zijn geweest.

Op 25 oktober 2017 is de [VERTROUWELIJK] van UBV op de hoogte geraakt van, wat Uber noemt, een "*IT security incident in 2016, that it was being investigated, and that it could potentially create a media cycle.*"

[3] Rapport van 10 januari 2018, [VERTROUWELIJK].

Op 4 november 2017 heeft een bespreking plaatsgevonden tussen UTI en UBV. Tijdens deze bespreking heeft UTI kenbaar gemaakt dat er sprake was van een beveiligingsincident.

Op 21 november 2017 is op de website van Uber een nieuwsbericht gepubliceerd door de huidige CEO van UTI waarin het publiek wordt ingelicht over het datalek.[4] Op diezelfde dag heeft UBV melding gedaan van een datalek aan de AP.

2. Wettelijk kader

Ten tijde van het datalek van 13 oktober 2016 tot 15 november 2016 en op het moment van de melding door UBV aan de AP op 21 november 2017, gold de Wbp, waaronder de meldplicht datalekken zoals neergelegd in artikel 34a, eerste en tweede lid, van de Wbp. De Wbp, die de implementatie vormde van richtlijn 95/46/EG[5], is ingetrokken op 25 mei 2018.[6] Op die dag is ook de Algemene Verordening Gegevensbescherming (AVG) van toepassing geworden[7] en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) in werking getreden.[8]
In subparagraaf 2.1 zal eerst het wettelijk kader onder de Wbp, voor zover relevant, worden beschreven en toegelicht. Vervolgens wordt in subparagraaf 2.2 het wettelijk kader onder de AVG, voor zover relevant, beschreven.

2.1 Wbp

2.1.1 Verwerking van persoonsgegevens

Artikel 1, aanhef en onder a, van de Wbp bepaalt dat een persoonsgegeven elk gegeven is betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Het begrip persoonsgegevens moet ruim worden opgevat. Om te bepalen of een natuurlijke persoon identificeerbaar is "*moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren*".[9]

Artikel 1, aanhef en onder b, van de Wbp bepaalt dat een verwerking van persoonsgegevens elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens is, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling,

[4] Zie https://www.uber.com/newsroom/2016-data-incident/
[5] Richtlijn van het Europees Parlement en de Raad van 24 oktober 1995, Publicatieblad van de Europese Gemeenschappen, 23 november 1995, Nr. L 281/31 (de zogenoemde Privacy richtlijn).
[6] In artikel 51 van de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) – die in werking is getreden met ingang van 25 mei 2018 – staat dat de Wbp wordt ingetrokken.
[7] Artikel 99, tweede lid, van de AVG bepaalt dat de AVG van toepassing is met ingang van 25 mei 2018.
[8] Bij koninklijk besluit van 16 mei 2018 (Staatsblad 2018, 145) is het tijdstip tot vaststelling van inwerkingtreding van de UAVG vastgesteld op 25 mei 2018. Dit besluit is gebaseerd op artikel 53 van de UAVG waarbij de inwerkingtreding van de UAVG op een bij koninklijk besluit te bepalen tijdstip mogelijk is gemaakt.
[9] Overweging 26 Richtlijn 95/46/EG (Richtlijn Bescherming Persoonsgegevens).

samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

2.1.2 Verantwoordelijke

Artikel 1, aanhef en onder d, van de Wbp bepaalt dat de verantwoordelijke de natuurlijke persoon, rechtspersoon of ieder ander is die of het bestuursorgaan is dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Het Hof van Justitie van de Europese Unie (HvJEU) heeft in een recent arrest bevestigd dat eventuele gezamenlijke verantwoordelijkheid voor bepaalde gegevensverwerkingen niet afdoet aan de individuele verantwoordelijkheid van één van de (gezamenlijke) verantwoordelijken.[10]

2.1.3 Toepassingsbereik Wbp

Artikel 4, eerste lid , van de Wbp bepaalt dat de Wbp van toepassing is op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland.

Artikel 4, tweede lid, van de Wbp bepaalt dat de Wbp van toepassing is op de verwerking van persoonsgegevens door of ten behoeve van een verantwoordelijke die geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens.

2.1.4 Beveiligingsverplichting

Artikel 13 van de Wbp bepaalt dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.[11]

2.1.5 Meldplicht datalekken

Per 1 januari 2016[12] bepaalt artikel 34a, eerste lid, van de Wbp dat de verantwoordelijke het College (lees: de AP) onverwijld in kennis stelt van een inbreuk op de beveiliging, bedoeld in artikel 13 van de Wbp, die

[10] HvJ EU, C-131/12 (Google Spain SL en Google Inc./Agencia Española de Protección de Datos (AEP)), 13 mei 2014, ro. 40. De Advocaat-Generaal Bot (AG) van het HvJEU heeft in een recente Conclusie betoogd dat 'gezamenlijke verantwoordelijkheid' in de zin van de Richtlijn ruim opgevat kan worden, in de zin dat er diverse varianten en taakverdelingen mogelijk zijn en ook dat bij het vaststellen van de verdeling van verantwoordelijkheden in juridische zin de wijze waarop entiteiten in de praktijk feitelijk samenwerken een doorslaggevend criterium is. Zie: Conclusie AG Bot, zaak C-210/16 (Wirtschaftsakademie Schleswig-Holstein), 24 oktober 2017, par. 46-51 en het daaropvolgende arrest HvJ EU, C-210/16, 5 juni 2018, ECLI:EU:C:2018:388.

[11] De AP (destijds het College bescherming persoonsgegevens) heeft in haar Richtsnoeren beveiliging van persoonsgegevens nader uitgewerkt wat onder 'passende technische en organisatorische beveiligingsmaatregelen' moet worden verstaan. Daarbij is aangesloten op standaarden, methoden en maatregelen die in het vakgebied informatiebeveiliging gebruikelijk zijn. Zie CBP Richtsnoeren Beveiliging van persoonsgegevens, februari 2013, URL: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-richtsnoeren-beveiliging-van-persoonsgegevens.

[12] Koninklijk besluit van 1 juli 2015 (*Stb.* 2015, 281).

leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Artikel 34a, tweede lid, van de Wbp bepaalt dat de verantwoordelijke, de betrokkene onverwijld in kennis stelt van de inbreuk, bedoeld in artikel 34a, eerste lid, van de Wbp, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

De AP heeft in haar Beleidsregels meldplicht datalekken verder uitgewerkt hoe verantwoordelijken invulling moeten geven aan de meldplicht datalekken, en geeft handvatten aan verantwoordelijken om te bepalen of zij bepaalde beveiligingsincidenten onder de meldplicht datalekken aan de AP moeten melden.[13] De Beleidsregels meldplicht datalekken bevatten ook een invulling van de meldplicht aan betrokkenen. De Beleidsregels meldplicht datalekken bepalen onder meer dat 'onverwijld', zoals bedoeld in artikel 34a, eerste lid, van de Wbp, melding binnen 72 uur betekent.

2.1.6 Bestuurlijke boete

Artikel 66, tweede lid, van de Wbp bepaalt, voor zover relevant, dat de AP een bestuurlijke boete kan opleggen van ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht ter zake van overtreding van het bepaalde bij artikel 34a van de Wbp. Artikel 23, zevende lid, van het Wetboek van Strafrecht is van overeenkomstige toepassing.

Artikel 66, derde lid, van de Wbp bepaalt, voor zover relevant, dat de AP geen bestuurlijke boete oplegt wegens overtreding van het bepaalde bij of krachtens de in artikel 66, tweede lid, van de Wbp genoemde artikelen, dan nadat het een bindende aanwijzing heeft gegeven. De AP kan de overtreder een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd.

Artikel 66, vierde lid, Wbp bepaalt, dat het derde lid niet van toepassing is indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid.

2.2 AVG

2.2.1 Melding van een inbreuk in verband met persoonsgegevens aan de AP

Artikel 33, eerste lid, van de AVG bepaalt, dat indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, de verwerkingsverantwoordelijke deze zonder onredelijke vertraging meldt 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 in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

[13] Beleidsregels *'De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)'* van 8 december 2015 (*Stcrt.* 2015, nr 46128).

Artikel 33, tweede lid, van de AVG bepaalt dat de verwerker de verwerkingsverantwoordelijke zonder onredelijke vertraging informeert zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

2.2.2 Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene

Artikel 34, eerste lid, van de AVG bepaalt dat wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee deelt.

2.2.3 Bestuurlijke boete

Artikel 83, eerste lid, van de AVG bepaalt dat elke toezichthoudende autoriteit ervoor zorgt dat de administratieve geldboeten die uit hoofde van dit artikel worden opgelegd voor de in de leden 4, 5 en 6 vermelde inbreuken op deze verordening in elke zaak doeltreffend, evenredig en afschrikkend zijn.

Artikel 83, vierde lid, van de AVG bepaalt dat op inbreuken van de artikelen 33 en 34 een administratieve geldboete kan worden opgelegd tot € 10.000.000 of, voor een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

3. Beoordeling

In deze paragraaf wordt in subparagraaf 3.1. eerst ingegaan op de bevoegdheid van de AP. Vervolgens wordt in subparagraaf 3.2 de verantwoordelijkheid voor de gegevensverwerking uiteengezet. De overtreding van artikel 34a, eerste lid, van de Wbp wordt in subparagraaf 3.3 vastgesteld. De overtreding van artikel 34a, tweede lid, van de Wbp wordt in subparagraaf 3.4 vastgesteld waarna in subparagraaf 3.5 de ernstig verwijtbare nalatigheid aan bod komt.

3.1 Bevoegdheid Autoriteit Persoonsgegevens

3.1.1 Periode van de gedraging

Van 13 oktober 2016 tot 15 november 2016 was er bij het Uber-concern een datalek.[14] Hiervan is UTI op 14 november 2016 op de hoogte gesteld. Op 21 november 2017 heeft UBV dit datalek bij de AP gemeld, waarna de AP - op grond van artikel 60 van de Wbp - is gestart met een onderzoek. Op 23 november 2017 heeft de AP een eerste schriftelijk informatieverzoek aan UBV gericht. De uiteindelijke de onderzoeksbevindingen van het onderzoek zijn opgenomen in het rapport van 1 juni 2018. Dat rapport en de zienswijze van Uber op het voornemen tot het opleggen van een bestuurlijke boete hebben geresulteerd in het onderhavige besluit. De AP is bevoegd naar aanleiding van vorenbedoeld datalek handhavend op te treden en daarmee onderhavig besluit te nemen. Hierna licht zij dat toe.

[14] In subparagraaf 3.3 'meldplicht datalek aan AP' wordt dit gemotiveerd.

3.1.2 AVG als boetegrondslag

Ten tijde van het datalek van 13 oktober 2016 tot 15 november 2016 en op het moment van de melding door UBV op 21 november 2017 gold de Wbp. De Wbp, die de implementatie vormde van richtlijn 95/46/EG[15], is ingetrokken op 25 mei 2018.[16] Op die dag is ook de AVG van toepassing geworden[17] en de UAVG in werking getreden.[18]

De AVG vervangt richtlijn 95/46/EG[19] en de Wbp. Daar waar de AVG ruimte geeft om nadere regels te stellen, zijn deze neergelegd in de UAVG. Blijkens de overwegingen bij de AVG blijven de doelstellingen en beginselen van richtlijn 95/46/EG gehandhaafd.[20] Zowel de richtlijn 95/46/EG als de Wbp en de AVG beogen de bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met verwerkingsactiviteiten en het vrije verkeer van persoonsgegevens binnen de Unie te waarborgen. De materiële normen waaraan de verwerking van persoonsgegevens onder het regime van de AVG moeten voldoen, zijn - in grote lijnen - ook gelijk gebleven aan die uit richtlijn 95/46/EG en de Wbp.

In dit geval is van belang dat zowel onder het regime van de Wbp als dat van de AVG sprake is van een meldplicht voor datalekken[21] en dat het niet naleven van de meldplicht beboetbaar is. In de Wbp is de meldplicht neergelegd in 34a, eerste en tweede lid, van de Wbp en in de AVG in artikel 33, eerste lid en artikel 34, eerste lid. Deze bepalingen beogen dezelfde rechtsbelangen te waarborgen. De bevoegdheid tot oplegging van een bestuurlijke boete vanwege een datalek is in de Wbp geregeld in artikel 66, tweede lid, van de Wbp en in de AVG in artikel 58, tweede lid, aanhef en onder i, in samenhang gelezen met artikel 83, vierde lid, van de AVG. Van een (wezenlijke) materiële wijziging van de regelgeving is geen sprake. Ook wordt niet anders gedacht over de strafwaardigheid van de meldplicht als zodanig.[22] Daarmee is sprake van een ononderbroken rechtsorde. Dit betekent dat, ter waarborging van de continuïteit van de rechtsorde, voor gedragingen die - zoals in onderhavig geval - plaatsvonden onder het regime van richtlijn 95/46/EG en de Wbp, de naleving moet worden verzekerd van de rechten en plichten zoals die golden onder dat regime.[23]

---

[15] Richtlijn van het Europees Parlement en de Raad van 24 oktober 1995, Publicatieblad van de Europese Gemeenschappen, 23 november 1995, Nr. L 281/31 (de zogenoemde Privacy richtlijn).
[16] In de UAVG – die in werking is getreden met ingang van 25 mei 2018 – staat in artikel 51 dat de Wbp wordt ingetrokken.
[17] Artikel 99, tweede lid, van de AVG bepaalt dat de AVG van toepassing is met ingang van 25 mei 2018.
[18] Bij koninklijk besluit van 16 mei 2018 (Staatsblad 2018, 145) is het tijdstip tot vaststelling van inwerkingtreding van de UAVG vastgesteld op 25 mei 2018. Dit besluit is gebaseerd op artikel 53 van de UAVG waarbij de inwerkingtreding van de UAVG op een bij koninklijk besluit te bepalen tijdstip mogelijk is gemaakt.
[19] In artikel 94 van de AVG wordt richtlijn 95/46/EG met ingang van 25 mei 2018 ingetrokken.
[20] Vgl. overweging 9 van de AVG.
[21] Hoewel richtlijn 95/46/EG geen regeling bevatte over een meldplicht van datalekken, blijkt uit de wetgeschiedenis betreffende de invoering van de meldplicht in de Wbp dat de wetgever, onder verwijzing naar de erkenning door de Europese Unie van de bescherming van persoonsgegevens als een fundamenteel recht, zoals blijkend uit onder andere richtlijn 95/46/EG, een regeling voor de meldplicht van datalekken als een dwingende eis van algemeen belang beschouwde. Uit de wetsgeschiedenis blijkt verder dat met de invoering van de meldplicht werd beoogd verwerkingen van persoonsgegevens in strijd met richtlijn 95/46/EG tegen te gaan (*Kamerstukken II* 2012/13, 33 662, nr. 3 Herdruk, p. 14.)
[22] Wel is sprake van een gewijzigde strafbedreiging.
[23] De AP wijst in dit verband op de Europeesrechtelijke jurisprudentie dienaangaande. Vgl. HvJEU 29 maart 2011 inzake ThyssenKrupp (C-352/09 P), HvJEU 18 juli 2007 inzake Lucchini (C-119/05) alsmede het arrest van het Hof van Justitie van 25 februari 1969 inzake Klomp (Zaak 23-68).

In een geval waarin de continuïteit van de rechtsorde aan de orde is, wordt, voor zover hier van belang, getoetst aan het materiële recht zoals dat gold op het moment waarop de gedraging[24] plaatsvond.[25] In dit geval is dat de Wbp, meer specifiek artikel 34a, eerste en tweede lid. Dit betekent ook dat wordt aangesloten bij het voor de overtreder in vergelijking met de AVG 'gunstiger' boeteregime onder de Wbp.[26] Onder de AVG kan een overtreding van de meldplicht immers worden beboet tot €10.000.000 of, indien dit hoger is, tot 2% van de totale wereldwijde jaaromzet[27] terwijl onder het regime van de Wbp dit, gelet op artikel 66, tweede, derde en vierde lid, van de Wbp, in beginsel ten hoogste € 820.000 was.[28]

Op grond van de AVG kan de meldplicht worden beboet op grond van artikel 58, tweede lid, aanhef en onder i, in samenhang bezien met artikel 83, vierde lid, sub a. Zoals de AP in dit besluit nader uiteen zet, zou onderhavige gedraging - en welke gedraging in dit besluit als overtreding van artikel 34a, eerste en tweede lid, van de Wbp is gekwalificeerd - als die zich zou hebben voorgedaan onder het regime van de AVG een overtreding van de artikelen 33, eerste lid en 34, eerste lid, van de AVG hebben opgeleverd.

3.1.3 Wbp als bevoegdheidsgrondslag; overgangsrecht UAVG

In artikel 48, achtste lid, van de UAVG is voorzien in overgangsrecht. Op grond van die bepaling is op wettelijke procedures en rechtsgedingen waar het College bescherming persoonsgegevens[29] voorafgaand aan de inwerkingtreding van de UAVG is betrokken, het recht van toepassing zoals dit gold voorafgaand aan de inwerkingtreding van de UAVG.

Voor zover het doen van onderzoek een wettelijke procedure is als bedoeld in artikel 48, achtste lid, van de UAVG dan ontleend de AP de bevoegdheid om een bestuurlijke boete op te leggen ook aan de Wbp. Het gaat dan om een wettelijke procedure waarbij de AP voorafgaand aan de inwerkingtreding van de UAVG - dus vóór 25 mei 2018 - betrokken is geraakt. Deze wettelijke procedure loopt door na intrekking van de Wbp en het van toepassing worden van de AVG en de inwerkingtreding van de UAVG. Ook het door de AP opgestelde rapport van 1 juni 2018 en (de procedure die heeft geleid tot) onderhavig besluit zijn onderdeel

[24] Waarbij wordt opgemerkt dat een gedraging mede een nalaten omvat zoals in onderhavig geval het niet onverwijld melden van een datalek.
[25] Wederom zij verwezen naar de Europeesrechtelijke jurisprudentie op dit vlak. Vgl. HvJEU 29 maart 2011 inzake ThyssenKrupp (C-352/09 P), punt 79 en Gerecht van eerste aanleg van de EG van 12 september 2007 inzake González y Díez, SA, SA (T-25/04), punt 59.
[26] In artikel 5:46, vierde lid, van de Awb wordt artikel 1, tweede lid, van het Wetboek van Strafrecht van overeenkomstige toepassing verklaard. Op grond van artikel 1, tweede lid, van het Wetboek van Strafrecht worden bij verandering in de wetgeving na het tijdstip waarop het feit begaan is, de voor de verdachte gunstigste bepalingen toegepast. Deze bepaling geeft uitdrukking aan de erkenning van het legaliteitsbeginsel voor het (materieel) strafrecht. Ook op veranderingen van wetgeving met betrekking tot de strafbedreiging geldt dat op basis van het zogenoemde Scoppola-arrest van het EHRM (EHRM 17 september 2009, ECLI:CE:ECHR:2009:0917JUD001024903) en het Arrest van de Hoge Raad van 12 juli 2011 (ECLI:NL:HR:2011:BP6878, *N*/2012/78) de meest gunstige bepaling moet worden toegepast.
[27] Artikel 83, vierde lid, aanhef en onder a, van de AVG.
[28] Alleen als dat niet zou leiden tot een passende bestraffing, kan de hoogte van de boete worden vastgesteld op ten hoogste tien procent van de jaaromzet van de rechtspersoon in het voorafgaande boekjaar. Bovendien kon onder het regime van de Wbp pas een boete worden opgelegd vanwege een datalek nadat een bindende aanwijzing was gegeven, tenzij de overtreding opzettelijk was gepleegd of het gevolg was van ernstig verwijtbare nalatigheid.
[29] Formeel is eerst bij de UAVG de naamswijziging van College bescherming persoonsgegevens naar Autoriteit Persoonsgegevens doorgevoerd hoewel de naam Autoriteit Persoonsgegevens in het maatschappelijk verkeer al langer wordt gevoerd.

van deze wettelijke procedure. Dat betekent dat op grond van het overgangsrecht in de UAVG de Wbp in dit geval van toepassing is en de AP ter zake van de overtreding van artikel 34a, eerste lid, van de Wbp - het niet onverwijld melden aan de AP van een datalek - bevoegd is op grond van artikel 48, achtste lid, van de UAVG in samenhang met artikel 66, tweede lid, van de Wbp een bestuurlijke boete op te leggen.

3.1.4 Conclusie ten aanzien van de bevoegdheid

Vorenstaande leidt tot de conclusie dat de AP haar bevoegdheid ontleent aan artikel 58, tweede lid, aanhef en onder i, in samenhang met artikel 83, vierde lid, sub a van de AVG[30] wegens overtreding van de meldplicht bedoeld in artikel 34a, eerste lid, van de Wbp en zoals sinds 25 mei 2018 is opgenomen in artikel 33, eerste lid en artikel 34, eerste lid van de AVG.

3.2 Verantwoordelijke voor de gegevensverwerking

3.2.1 Inleiding

Hiervoor is uiteengezet dat UBV en UTI ten behoeve van hun dienstverlening persoonsgegevens in de zin van de Wbp verwerken. In het kader van de vraag of is voldaan aan de meldplicht als bedoeld in artikel 34a, eerste lid en tweede lid, van de Wbp is van belang wie is aan te merken als verantwoordelijke. De verantwoordelijke is immers de normadressaat.

Onder 'verantwoordelijke' in de zin van artikel 1, aanhef, en onder d, van de Wbp, wordt verstaan:

> *'de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;'* [31]

Uit de rechtspraak van het Hof van Justitie van de Europese Unie volgt dat het doel van deze bepaling - die de implementatie vormt van het begrip 'voor de verwerking verantwoordelijke' uit artikel 2, onder d, van richtlijn 95/46/EG - erin bestaat een doeltreffende en volledige bescherming van de betrokkenen te verzekeren via een *ruime* omschrijving van het begrip 'verantwoordelijke'.[32]

In dit verband wordt nog opgemerkt dat de AVG in artikel 4, zevende lid, de 'verwerkingsverantwoordelijke' (materieel) gelijkwaardig definieert als richtlijn 95/46/EG en de Wbp.

3.2.2 UBV formeel-juridische verantwoordelijke

Bij de beantwoording van de vraag wie verantwoordelijke is, speelt de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen een belangrijke rol.[33] Ingeval van concernverhoudingen, zoals hier aan de orde, wordt de rechtspersoon onder wiens bevoegdheid de

[30] Deze bevoegdheid is nationaalrechtelijk verankerd in artikel 14, derde lid, van de UAVG.
[31] Deze omschrijving, komt voor zover relevant, overeen met de definitie van 'voor de verwerking verantwoordelijke' uit artikel 2, onder d, van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
[32] HvJ EU 13 mei 2014, Google Spain, SL, C-131/12 9, punt 34 (ECLI:EU:C:2014:317) en HvJ EU 5 juni 2018, Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16, punt 28 (ECLI:EU:C:2018:388).
[33] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 55.

operationele gegevensverwerking plaatsvindt als de verantwoordelijke gezien.[34] In de bewerkersovereenkomst van 31 maart 2016 ('Data Processing Agreement') tussen UBV en onder meer UTI, wordt UBV aangemerkt als verantwoordelijke ('controller'[35]) voor de verwerking van (persoons)gegevens die zij verzamelt en verwerkt van betrokkenen buiten de Verenigde Staten, waaronder betrokkenen in Europa. UTI wordt daarin vervolgens aangemerkt als bewerker ('processor')[36] die ten behoeve van UBV persoonsgegevens verwerkt.[37] De AP is van oordeel dat hieruit afgeleid kan worden dat UBV de formeel-juridische bevoegdheid heeft om doel en middelen van de gegevensverwerking vast te stellen en daarmee als verantwoordelijke in de zin van artikel 1, aanhef, en onder d, van de Wbp kan worden aangemerkt. Dit sluit, zoals hierna nader wordt gemotiveerd, overigens niet uit dat naast UBV ook UTI als verantwoordelijke kan worden aangemerkt.

3.2.3 UBV en UTI zijn gezamenlijk verantwoordelijke

De AP is van oordeel dat UBV niet alleen, maar tezamen met UTI doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. UBV en UTI zijn daarmee als gezamenlijk verantwoordelijke aan te merken. Elk van de verantwoordelijken, zowel UTI als UBV, is aansprakelijk voor het geheel van de gegevensverwerking en de naleving van de daarmee samenhangende verplichtingen.[38] Hierna motiveert de AP dat standpunt en betrekt daarbij ook de zienswijze van Uber op het rapport van de AP. Uber zelf beschouwt UBV als de - enige - verantwoordelijke.[39]

De verantwoordelijke is de organisatie die het doel van en de middelen voor de gegevensverwerking bepaalt. Hij kan dit alleen doen, maar ook samen met anderen. De AP is van oordeel dat UBV en UTI zijn te beschouwen als gezamenlijk verantwoordelijke.

Hoewel UBV op grond van de bewerkersovereenkomst de formeel-juridisch zeggenschap heeft, is dat niet per definitie doorslaggevend voor de vraag of UBV (alleen) verantwoordelijke is. Zoals de Artikel 29-werkgroep - het onafhankelijke advies- en overleg orgaan van Europese privacy toezichthouders en thans de European Data Protection Board geheten - in haar advies van 16 februari 2010[40] opmerkt, geven de bepalingen in een contract vaak meer duidelijkheid, maar zij zijn niet altijd doorslaggevend. Het begrip 'voor de verwerking verantwoordelijke' is een functioneel begrip, bedoeld om verantwoordelijkheden te leggen op de plaats waar de feitelijke invloed ligt.[41] Op grond van deze feitelijke beoordeling, oordeelt de AP dat UTI en UBV (gezamenlijk) beslissingen nemen met betrekking tot de vaststelling van doelen en middelen voor de gegevensverwerking.

---

[34] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 56.
[35] In de Engelse tekst van Richtlijn 95/46 wordt voor verantwoordelijke de term 'controller' gebruikt.
[36] In de Engelse tekst van Richtlijn 95/46 wordt voor verwerker (in Wbp-terminologie de bewerker) de term 'processor' gebruikt.
[37] Zie inleidende overwegingen in de bewerkersovereenkomst (met name overwegingen A t/m D).
[38] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 58. Het gaat daarmee om de derde vorm van verantwoordelijkheid die de wetgever voor ogen heeft gehad.
[39] Schriftelijke reactie Uber van 1 december 2017, p. 5, antwoord op vraag 1 alsmede de zienswijze Uber van 3 juli 2018, p. 6.
[40] Werkgroep "Artikel 29", Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", p. 14.
[41] Werkgroep "Artikel 29", Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", p. 11 alsmede conclusie AG Jääskinen 25 juni 2013 inzake Google Spain en Google (Zaak C-131/12), punt 83 en AG Bot van 24 oktober 2017 inzake Wirtschaftsakademie Schleswig-Holstein GmbH (Zaak C-210/16), punt 46.

Ten aanzien van UTI gaat het om:

- Het gezamenlijk vaststellen van het doel van de gegevensverwerking;
- Vaststelling van het informatiebeveiligingsbeleid;
- Beslissingen over opslag van de gegevens, en
- De ontwikkeling en het aanbieden van de Uber-app alsmede het uitvoeren van updates.

Deze factoren zullen hierna worden toegelicht.

Gezamenlijk vaststellen van het doel van de gegevensverwerking; uniform privacybeleid
UBV en UTI stellen primair het doel van de verwerking van de persoonsgegevens vast. In de brief van 7 februari 2018 verklaart Uber dat het opstellen van de privacyverklaring een gezamenlijke inspanning is geweest van UBV en UTI.[42] Uit de inleidende paragraaf van de privacyverklaring blijkt dat de privacyverklaring van toepassing is op zowel persoonsgegevens die in de Verenigde Staten als daarbuiten worden verzameld. Het heeft daarmee een wereldwijd toepassingsbereik. In de privacyverklaring, onder *'Use of Information'* staat voor welke doeleinden de informatie kan worden verwerkt. De door de gebruikers verstrekte informatie, waaronder persoonsgegevens, worden gebruikt met het doel om:

- dienstverlening mogelijk te maken, te onderhouden en te verbeteren;
- interne werkzaamheden uit te voeren;
- berichten te sturen of communicatie mogelijk te maken;
- berichten te sturen waarvan Uber meent dat zij interessant zijn voor de gebruikers;
- diensten te personaliseren en te verbeteren.

Van de persoonsgegevens die door het Uber-concern worden verwerkt, worden back-ups gemaakt die worden opgeslagen in haar AWS S3 opslag in de Verenigde Staten.[43] De verwerking van persoonsgegevens voor het maken van back-ups vindt plaats in het kader van het reguliere (dagelijkse) bedrijfsproces van het Uber-concern en is als zodanig aan te merken als onderdeel van de normale dienstverlening aan gebruikers van de Uber app. Het datalek zag op persoonsgegevens in de back-ups opgeslagen in de (externe) AWS S3 opslag.[44]

Uit het vorenstaande concludeert de AP dat UTI en UBV 'te zamen' het doel van de verwerking van persoonsgegevens vaststellen. In het advies van 16 februari 2010 van de Artikel 29-werkgroep staat dat wie het doel van de verwerking vaststelt in ieder geval als voor de verwerking verantwoordelijk wordt aangemerkt.[45] Nu uit het voorgaande blijkt dat UTI en UBV gezamenlijk het doel van de verwerking van persoonsgegevens vaststellen, zijn zij reeds op die grond gezamenlijk verantwoordelijke.

[42] Schriftelijke reactie Uber van 7 februari 2018, p. 3. Het Uber-concern kende zowel een privacyverklaring voor gebruikers ('users') als voor chauffeurs ('drivers') en waren gedateerd 15 juli 2015 met (nagenoeg) identieke doeleinden.
[43] Zie nader paragraaf 4.2.4, p. 18, van het rapport.
[44] Zie nader paragraaf 4.3.3, p. 22, van het rapport.
[45] Werkgroep "Artikel 29", Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", p. 17.

Informatiebeveiligingsbeleid
Naast het doel stelt UTI ook (mede) de middelen vast voor de verwerking. Daarbij is van belang op te merken dat ook als iemand louter de middelen vaststelt, hij verantwoordelijke kan zijn. De Artikel 29-werkgroep geeft in haar voornoemd advies aan dat bij het vaststellen van de middelen alleen van verantwoordelijkheid sprake is wanneer die vaststelling betrekking heeft op de wezenlijke aspecten van de middelen.[46]

Het Uber-concern, waar UBV en UTI deel van uitmaken, hanteert een wereldwijd informatiebeveiligingsbeleid (Information Security Policy) geldend voor alle entiteiten van het Uber-concern. Dit beleid, waarin onder meer beveiligingsmaatregelen ten aanzien van de bescherming van informatie en (persoons)gegevens zijn opgenomen, is vastgesteld door UTI.[47] Daarbij gaat het bijvoorbeeld om maatregelen ten aanzien van versleuteling, beveiligingsprocedures op gebied van (rechten tot)toegang tot informatie[48] en beveiligingseisen voor de informatiesystemen van Uber. Uit het informatiebeveiligingsbeleid blijkt ook dat de [VERTROUWELIJK] van UTI verantwoordelijk is voor alle aspecten van de beveiliging van informatie, waaronder persoonsgegevens. Het informatiebeveiligingsbeleid vermeldt in dit verband: "*Uber's information security training, guidance, direction, and authority shall be delegated to the* [VERTROUWELIJK]."[49] Het gaat hier dus niet alleen om technische of organisatorische zaken die op zich aan een bewerker zouden kunnen worden gedelegeerd.[50]

De AP is van oordeel dat UTI hiermee een wezenlijk aspect van de middelen vaststelt en dit (mede) eraan bijdraagt dat UTI samen met UBV het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[51] Niettemin benadrukt de AP dat - zoals hiervoor uiteengezet - UTI (mede) het doel van de verwerking vaststelt en reeds daarom met UBV als gezamenlijk verantwoordelijke kan worden gekwalificeerd.

Zienswijze Uber en reactie AP
Over haar werkwijze merkt Uber in haar zienswijze op dat de verantwoordelijke bepaalt hoe en waarom persoonsgegevens worden verwerkt. Dat de bewerker een zekere beoordelingsvrijheid heeft over details van de uitvoering van de verwerking, maakt de bewerker, zo betoogt Uber, nog geen verantwoordelijke.

---

[46] Werkgroep "Artikel 29", Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", p. 17.
[47] Dit kan worden opgemaakt uit het feit dat in de *Information Security Policy Version 1.0* van 9 maart 2014 op de voorpagina staat dat *"This document is the property of Uber Technologies, Inc."*. In de *Information Security Policy Version 0.1* van 31 augustus 2016 staat op de voorpagina als auteur *'Uber Inc.'* genoemd. In de inleiding wordt het document geïntroduceerd als "*The Uber Inc* ("*Uber*"or "*the company*") Information Security Policy". In de daaropvolgende versie van het informatiebeveiligingsbeleid van maart 2017 staat op de voorpagina UTI. In het informatiebeveiligingsbeleid dat gold ten tijde van het door UBV gemelde datalek, wordt vermeld: *"Uber's information security training, guidance, direction, and authority shall be delegated to the Chief Security Officer (CSO)."*
[48] Zo wordt door de Artikel 29-werkgroep aangegeven dat de entiteit die bijvoorbeeld besluit voor wie de verwerkte gegevens toegankelijk moeten zijn als verantwoordelijke kan worden aangemerkt (advies 1/2010 op p. 18).
[49] Information Security Policy version 0.1, August 31, 2016, p. 5 (Zie ook rapport AP d.d. 1 juni 2018, paragaaf 4.2.3, p. 18).
[50] Vgl. advies Artikel 29-werkgroep 1/2010 op p. 18
[51] De Artikel 29-werkgroep merkt in haar advies 1/2010 op p. 17 op dat in sommige rechtsstelsels beveiligingsmaatregelen uitdrukkelijk als wezenlijk kenmerk worden beschouwd.

Uber verwijst hierbij naar de brief van het College Bescherming Persoonsgegevens (CBP) van 14 mei 2002 en de richtlijnen van de ICO.

De AP volgt deze zienswijze niet en merkt op dat het vaststellen van het beveiligingsbeleid niet als 'details van de uitvoering van de verwerking' kunnen worden beschouwd. De AP merkt op dat in de brief van het CBP uit 2002 in algemene termen wordt toegelicht dat voor de beantwoording van de vraag wie verantwoordelijke is, meer gewicht wordt toegekend aan het bepalen van de doeleinden van de verwerking dan aan het bepalen van de details van de verwerking en dat voor de afbakening verantwoordelijke/bewerker het bepalen van doeleinden van de verwerking en de zeggenschap doorslaggevend zijn. Uit de inhoud van deze brief kan naar het oordeel van de AP niet worden opgemaakt dat de wijze waarop met name UTI (feitelijk) opereert tot de conclusie zou moeten leiden dat UBV en UTI niet als gezamenlijk verantwoordelijke kunnen worden beschouwd. Integendeel, zoals hiervoor opgemerkt, bepaalt UTI mede het doel en de middelen van de verwerking.

Uber citeert in haar zienswijze verder nog een passage uit de richtlijnen van de ICO, waaruit volgens Uber blijkt dat een bewerker een zekere beoordelingsvrijheid heeft over details van de uitvoering van verwerking van gegevens. In de richtlijnen wordt een voorbeeld gegeven van een bank die een IT-bedrijf inschakelt voor de opslag van gegevens.
In reactie hierop merkt de AP op dat dit voorbeeld niet de conclusie rechtvaardigt dat UTI in dit geval niet als gezamenlijk verantwoordelijke kan worden aangemerkt. De rol van UTI gaat, zoals hierna uiteen wordt gezet, verder dan louter het verzorgen van de opslag zoals in het in de richtlijnen van de ICO aangehaalde voorbeeld. Bovendien wordt het zijn van gezamenlijk verantwoordelijke ook bepaald door het hanteren van een uniform privacy beleid en het door UTI vaststellen van het informatiebeveiligingsbeleid alsmede de hierna te bespreken ontwikkeling, aanbod en updates van de Uber-apps en de afhandeling van het datalek door UTI.

Opslag van de persoonsgegevens
De opslag van persoonsgegevens speelt een belangrijke rol bij de verwerking van persoonsgegevens. Ook ten aanzien van opslag neemt UTI belangrijke beslissingen en heeft zij een ruime mate van zeggenschap. Zo is het UTI die met Amazon een overeenkomst is aangegaan voor de opslag ten behoeve van back-ups.[52] Hierin is overeengekomen dat gebruik wordt gemaakt van de Amazon opslagdienst AWS S3. In dat verband is door UTI ook gekozen voor de Verenigde Staten als de locatie voor die opslag, waarbij [VERTROUWELIJK].

[52] Schriftelijke reactie UBV van 12 januari 2018, p. 6, antwoord op vraag 8.

Uit het vorenstaande maakt de AP op dat UTI zich ten aanzien van opslag van persoonsgegevens autonoom van UBV heeft opgesteld en een bepalende invloed heeft gehad op de wijze waarop de opslag - een middel voor de verwerking van persoonsgegevens - plaatsvindt. UTI heeft daarmee (feitelijk) een grote mate van zeggenschap gehad over de wijze waarop de verwerking van de persoonsgegevens plaatsvindt. Het was meer dan een louter ondersteunende rol en het maakt in combinatie met de andere feiten en omstandigheden - het hanteren van een uniform privacy beleid, het vaststellen van het informatiebeveiligingsbeleid alsmede de hierna te bespreken ontwikkeling, aanbod en updates van de Uber-apps, en de afhandeling van het datalek door UTI - dat UTI en UBV gezamenlijk verantwoordelijke zijn.

Zienswijze Uber en reactie AP
Uber stelt in haar zienswijze over de opslag het niet eens te zijn met de conclusie van de AP dat UTI de bepalende invloed van UTI op de locatie en de uitvoering van de gegevensopslag als indicator kan worden gezien om UTI aan te merken als verantwoordelijke voor de gegevensverwerking. Zij wijst erop dat de bewerkersovereenkomst opslag door UTI toestaat en dat UTI als bewerker ook een sub-bewerker (in dit geval Amazon) kan inschakelen. Daarbij heeft UTI ervoor gezorgd dat dezelfde verplichtingen gelden tussen UTI en Amazon als tussen UBV en UTI. Dat is volgens UTI ook een gebruikelijke constructie.

Dienaangaande merkt de AP op dat de omstandigheid dat de opslag van persoonsgegevens door UTI mogelijk is op basis van de bewerkersovereenkomst en een bewerker ook gebruik mag maken van een sub-bewerker, dit niet betekent dat beslissingen die UTI feitelijk heeft genomen over de opslag van persoonsgegevens - en in combinatie met de andere genoemde feiten en omstandigheden - daarmee irrelevant zouden zijn voor de vraag of UBV en UTI als gezamenlijk verantwoordelijke kunnen worden aangemerkt. De AP is van oordeel dat dat niet het geval is. In dit verband benadrukt de AP dat UTI voormelde beslissingen ten aanzien van de opslag zelfstandig heeft genomen zonder UBV daarin te kennen. Het neemt niet weg dat het type beslissingen en het autonome optreden van UTI in combinatie met de overige hiervoor genoemde feiten en omstandigheden een rol spelen bij de beoordeling dat UBV en UTI gezamenlijk verantwoordelijke zijn.

Ontwikkeling, aanbod en updates Uber-app
Het Uber-concern biedt een dienst aan die het voor gebruikers mogelijk maakt om via een speciaal daartoe ontwikkelde app (Uber app) personenvervoer af te nemen. Gebruikers worden gekoppeld aan een chauffeur (driver) die via een andere app (Uber Driver app) klanten kunnen aannemen. De speciaal ontwikkelde mobiele applicaties vormen in wezen de kerndienst van het Uber-concern.[53] UTI[54] heeft de Uber app - die als basis geldt voor andere apps – ontwikkeld en heeft UBV de licentie gegeven om de app te exploiteren, terwijl ook de updates van de Uber-app door UTI worden uitgevoerd. [55] Daarmee draagt UTI bij aan de vaststelling van doel en middelen voor de verwerking van persoonsgegevens.[56] Verder is UTI ook de aanbieder van de Uber-app in de Apple-App store en Google Play Store. Dat UBV - naar Uber in haar

[53] Vgl. inleidende overweging van de privacyverklaring voor gebruikers ('users') en voor chauffeurs ('drivers') van 15 juli 2015.
[54] En haar voorlopers.
[55] Vgl. verklaring van [VERTROUWELIJK], van UBV op p. 20 van het hoorzittingsverslag.
[56] Zie nader paragraaf 4.2.6, p. 19 van het rapport van de AP.

zienswijze stelt - verantwoordelijk is voor het toevoegen van nieuwe functionaliteiten, doet daar niet aan af. Het benadrukt veeleer de gezamenlijke verantwoordelijkheid. De omstandigheid dat UTI ontwikkelaar, aanbieder en uitvoerder van updates van de Uber app is, is nog steeds één van de elementen die relevant is voor de vraag of UBV en UTI als gezamenlijk verantwoordelijke kunnen worden aangemerkt. Dat geldt ook ten aanzien van het betoog van Uber in haar zienswijze dat de aanbieder van de app en de identiteit van de ontwikkelaar van de Uber app niet relevant, dan wel niet bepalend zijn voor wie bewerker of verantwoordelijke is.

Tussenconclusie gezamenlijke verantwoordelijkheid
Op grond van voornoemde omstandigheden concludeert de AP dat UBV en UTI gezamenlijk verantwoordelijke zijn.

De afhandeling van het datalek door UTI
De AP ziet zich in haar oordeel dat UTI en UBV gezamenlijk verantwoordelijke zijn, bevestigd en gesterkt door de autonome en onafhankelijke rol die UTI heeft genomen bij de afhandeling van het datalek. In dat verband merkt de AP op dat de feitelijke beslissingen over de afhandeling over het datalek - waarover UBV bijna een jaar nadat het datalek heeft plaatsgevonden, is geïnformeerd - zelfstandig en louter door het personeel van UTI zijn genomen. Er zijn door de [VERTROUWELIJK] van UTI, zonder hierin UBV te kennen en haar de gelegenheid te geven daarop invloed uit te oefenen, specifieke en gewichtige maatregelen genomen. Deze maatregelen zien op het versleutelen van bestanden in de AWS S3 buckets en het vereisen van twee-factorauthenticatie voor diensten waarvan het Uber-concern gebruik maakt en die bereikbaar zijn via het internet.[57]

De stelling van Uber in haar zienswijze dat het zelfstandig afhandelen door UTI van het datalek zonder UBV daarbij te betrekken alleen aantoont dat UTI de verplichtingen uit de overeenkomst niet is nagekomen, volgt de AP niet. Uber miskent hiermee dat deze feitelijke handelwijze juist de conclusie van de AP bevestigt dat UTI zelfstandig besluiten neemt en aldus feitelijk de zeggenschap heeft over de manier waarop een datalek wordt afgehandeld.

UTI heeft daarnaast - zo geeft Uber in nummer 2.23 van haar zienswijze aan - advocatenkantoor [VERTROUWELIJK]verzocht om [VERTROUWELIJK], een extern forensisch expert, in te schakelen. Ook hierin is UBV niet vooraf (of onverwijld daarna) gekend. Dat het volgens Uber - zoals zij in haar zienswijze stelt -logisch was dat UTI zelfstandig een onderzoek heeft gedaan omdat het incident betrekking had op meer Amerikaanse gebruikers dan Nederlandse gebruikers of dat van enig ander land en UTI de verantwoordelijke is voor de verwerking van persoonsgegevens van gebruikers in de Verenigde Staten, overtuigt niet. Het had volgens de AP voor de hand gelegen UBV te betrekken juist omdat het bij de opslag van persoonsgegevens in de Verenigde Staten ook gaat om persoonsgegevens die zijn verzamelt en verwerkt van betrokkenen buiten de Verenigde Staten en daarvoor is volgens de bewerkersovereenkomst UBV verantwoordelijk.[58]

[57] Zie daarover meer specifiek paragraaf 4.3.4 van het rapport en daar in de voetnoten 101 en 102 genoemde bronnen afkomstig van Uber.
[58] Schriftelijke reactie Uber van 7 februari 2018, p. 2, antwoord op vraag 1.

UTI heeft de melders van het datalek ten behoeve van de bescherming van gebruikersgegevens[59] een beloning betaald. Daarbij gaat het om een aanzienlijk groter bedrag dan gewoonlijk wordt betaald.[60] UBV is niet betrokken en niet gekend in de besluitvorming hierover. De in dit verband met de melders gesloten overeenkomst is door UTI personeel en namens UTI getekend. UBV stond daar buiten.

Zienswijze Uber en reactie AP
In haar zienswijze merkt Uber op dat de betaling aan de melders en de met hen gesloten overeenkomst geen indicatie is dat UTI verantwoordelijke is omdat het niets zegt over het vaststellen van de doeleinden van de verwerking van de gebruikersgegevens.
De AP volgt deze argumentatie niet. Door de [VERTROUWELIJK] van UTI is kenbaar gemaakt waarom deze betaling is gedaan: *"our primary goal in paying the intruders was to protect our consumers' data."* Het vormt met andere woorden een middel ter bescherming van de (persoons)gegevens van de klanten van het Uber-concern. Dat dit gebeurt door het betalen van een aanmerkelijk groter bedrag dan gebruikelijk en zonder UBV hierin te betrekken, laat bovendien zien dat UTI verder gaat dan van een bewerker mag worden verwacht.

Uber wijst er in haar zienswijze op dat de omstandigheid dat het personeel van UTI - zonder UBV te informeren - het datalek heeft afgehandeld en maatregelen heeft genomen, niet inhoudt dat UTI verantwoordelijke is.
De AP merkt daarover op dat de wijze waarop UTI feitelijk opereert en beslissingen neemt waar het de afhandeling van het datalek betreft, één van de factoren is die relevant is voor de vraag of UTI als gezamenlijk verantwoordelijke is aan te merken. De rol die UTI vervult bij de afhandeling van het incident staat daarmee niet op zichzelf.

3.2.4 Conclusie gezamenlijk verantwoordelijke
Gelet op het vorenstaande concludeert de AP dat UBV en UTI gezamenlijk verantwoordelijke zijn in de zin van artikel 1, aanhef, en onder d, van de Wbp. De AP heeft daarbij acht geslagen op de bewerkersovereenkomst, waarbij UBV als verantwoordelijke is aangemerkt. Verder is gebleken dat UTI samen met UBV het doel van de gegevensverwerking heeft vastgesteld, UTI zelf het informatiebeveiligingsbeleid heeft vastgesteld, zelfstandig belangrijke beslissingen heeft genomen ten aanzien van de opslag van persoonsgegevens en de Uber-app heeft ontwikkeld en die ook aanbiedt en daarvoor updates uitvoert. Het oordeel van de AP wordt verder versterkt door de zelfstandige manier waarop UTI het onderhavige datalek heeft afgehandeld. De gezamenlijke verantwoordelijkheid brengt met zich mee dat elk van de verantwoordelijken, dus zowel UTI als UBV, aansprakelijk is voor het geheel van de gegevensverwerking en de naleving van de daarmee samenhangende verplichtingen. In dit verband merkt de AP op dat ook onder het AVG-regime UTI en UBV als gezamenlijk verantwoordelijke kunnen worden aangemerkt.

3.3 Overtreding meldplicht datalek aan AP

[59] Schriftelijke reactie Uber van 7 februari 2018, bijlage "Testimony Uber (201826).pdf", p. 5.
[60] Zie nader paragraaf 4.3.5, p. 25-27, van het rapport van de AP.

3.3.1 Inleiding

Zoals uit subparagraaf 2.1.5 blijkt, gold per 1 januari 2016 op grond van artikel 34a, eerste lid, van de Wbp een meldplicht voor datalekken aan de AP. Ingevolge deze meldplicht dient de verantwoordelijke de AP onverwijld in kennis te stellen van een inbreuk op de beveiliging, bedoeld in artikel 13, van de Wbp, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige heeft voor de bescherming van persoonsgegevens. Met deze meldplicht wordt bijgedragen aan het behoud en herstel van vertrouwen van het publiek, de klanten, de markt, de overheid en de toezichthouders in de desbetreffende instelling of het desbetreffende bedrijf bij de omgang met persoonsgegevens.[61]

3.3.2 Verantwoordelijke is normadressaat

Hiervoor is gemotiveerd uiteengezet dat UBV en UTI als gezamenlijk verantwoordelijke zijn aan te merken. Beide zijn gezamenlijk verantwoordelijk voor de naleving van de Wbp voor het geheel van de verwerking. Op zowel UBV als UTI rust daarmee de plicht onverwijld melding te doen van een datalek waarop artikel 34a, eerste lid, van de Wbp betrekking had. De stelling van Uber in haar zienswijze dat de meldplicht niet op UTI van toepassing is omdat UTI geen verantwoordelijke is - en daarmee geen normadressaat - acht de AP dan ook onjuist.

3.3.3 Inbreuk op de beveiliging als bedoeld in artikel 13 Wbp

In artikel 34a, eerste lid, van de Wbp werd gerefereerd aan een inbreuk op de beveiliging als bedoeld in artikel 13 Wbp (thans artikel 32 van de AVG). Artikel 13 betrof een beveiligingsvoorschrift waaraan de verantwoordelijke zich moest houden en richtte zich tegen 'verlies of enige vorm van onrechtmatige verwerking' van persoonsgegevens. Onbevoegde kennisneming is een vorm van onrechtmatige verwerking[62] waartegen de beveiligingsmaatregelen bescherming moeten bieden. In onderhavige casus hebben, zoals hierna uiteen wordt gezet, onbevoegden van buiten het Uber-concern zich toegang tot de gegevensopslag van Uber verschaft. Zo konden zij bestanden downloaden waarmee zij toegang hadden tot, en kennis konden nemen van, persoonsgegevens. Aldus was sprake van een vorm van onrechtmatige verwerking.

Van 13 oktober 2016 tot 15 november 2016 waren persoonsgegevens die waren opgeslagen in de AWS S3 opslag van UTI toegankelijk voor onbevoegde personen van buiten het Uber-concern.

In haar zienswijze op pagina 18, onder 3.5, verklaart Uber uitdrukkelijk dat zij '*niet betwist dat in die periode van een inbreuk op de beveiliging in de zin van artikel 34a Wbp sprake was*'.[63] In dit verband wordt opgemerkt dat UTI forensisch expert [VERTROUWELIJK] onderzoek heeft laten doen naar dit datalek en haar bevindingen heeft gerapporteerd.[64] [VERTROUWELIJK] is gevraagd om te bepalen in hoeverre de

[61] Vgl. *Kamerstukken II* 2012/13, 33 662, nr. 3 Herdruk, p. 1 en 3.
[62] Vgl. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 98.
[63] De AP gaat er, gelet op het verdere betoog van Uber in haar zienswijze, vanuit dat Uber de inbreuk op de beveiliging als bedoeld in artikel 13 van de Wbp niet betwist.
[64] Rapport [VERTROUWELIJK]van 10 januari 2018 met nummer 138128103.1

onbevoegden toegang hadden tot de data die waren opgeslagen op de AWS S3 opslag:
"[VERTROUWELIJK] *was instructed to determine the extent of these outside actors' access to Uber's data stored on S3."*

[VERTROUWELIJK] heeft geconstateerd dat onbevoegden in totaal 16 bestanden uit de AWS S3 opslag van het Uber-concern hebben gedownload[65] en daarmee toegang hadden tot, en kennis konden nemen van, de daarin opgenomen gegevens. Volgens de onbevoegden konden zij toegang tot de zogenaamde private GitHub-repository van Uber krijgen door gebruikmaking van eerder gelekte gebruikersnamen en wachtwoorden. Hiermee konden zij uiteindelijk toegang krijgen tot vorenbedoelde AWS S3 bestanden[66]. Deze onbevoegden hebben voor het eerst op 13 oktober 2016 en voor het laatst op 15 november 2016 bestanden gedownload van deze AWS S3 opslag.[67] Het datalek heeft daarmee bijna vijf weken geduurd. Gedurende die periode konden in elk geval deze onbevoegden toegang krijgen tot persoonsgegevens van Uber klanten. Het ging daarbij onder meer om onversleutelde persoonsgegevens zoals voornaam, achternaam, e-mailadres en telefoonnummers van Nederlandse Uber-gebruikers.[68] Uber betwist overigens niet dat sprake was van een de inbreuk op de beveiliging. Daarmee was sprake van een inbreuk op de beveiliging als bedoeld in artikel 13 van de Wbp, zoals dat destijds gold.

UBV heeft ten aanzien van de Nederlandse Uber-gebruikers een representatieve selectie gemaakt van persoonsgegevens van tien Nederlandse riders en drivers zoals die in de back-ups van de databases zijn gedownload door de onbevoegden. Hieruit blijkt dat onder meer voornaam, achternaam, e-mailadres en telefoonnummers van Nederlandse Uber-gebruikers in de gedownloade database back-up aanwezig waren.[69]

3.3.4 Inbreuk heeft (aanzienlijke kans op) ernstige nadelige gevolgen

Ingevolge artikel 34a, eerste lid, van de Wbp is eerst sprake van een meldingsplichtige inbreuk op de beveiliging als die inbreuk *'leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens'*.

Omdat in dit geval onbevoegden bestanden van Uber op haar AWS S3 opslag hebben gedownload en daarmee toegang hadden tot, en kennis konden nemen van de daarin opgenomen persoonsgegevens van Uber klanten was sprake van een onrechtmatige verwerking en hebben de nadelige gevolgen voor de bescherming van persoonsgegevens zich daadwerkelijk gemanifesteerd. Reeds daarom is naar het oordeel van de AP sprake van ernstige nadelige gevolgen. Het gaat hier in de woorden van de memorie van

[65] Vgl. de bevindingen van [VERTROUWELIJK]zoals vastgelegd in haar rapport op p. 4 en 5. In het bij brief van 22 oktober 2018 nagestuurde addendum behorende bij het rapport van 10 januari 2018 is naar aanleiding van een analyse van aanvullende logboeken, die nadien nog aan [VERTROUWELIJK]door Uber zijn versterkt, door [VERTROUWELIJK]vastgesteld dat de onbevoegden buiten de 16 bestanden die zijn beschreven in het oorspronkelijke rapport van 10 januari 2018 geen andere bestanden zijn gedownload.
[66] Vgl. e-mailconversatie op 15 november 2016 van een medewerker van Uber en de melder (bijlage 3 bij de brief van Uber van 11 december 2017) alsmede paragraaf 3.9 van de zienswijze van Uber.
[67] Appendix b, tabel 3, p. 11 en 12 van het rapport van [VERTROUWELIJK].
[68] Vgl. Brief UBV 11 december 2017, bijlage 2, brief UBV 12 januari 2018 (reactie op vraag 17) en het [VERTROUWELIJK]rapport, p. 7 -9.
[69] Vgl. Brief UBV 11 december 2017, bijlage 2, brief UBV 12 januari 2018 (reactie op vraag 17) en het [VERTROUWELIJK]rapport, p. 7 -9.

toelichting om een 'geslaagde aanval van hackers', hetgeen op zichzelf al een belangrijke indicatie is dat sprake is van een meldingsplichtig datalek.[70]

Ten aanzien de omvang van de bij het datalek betrokken persoonsgegevens merkt de AP op dat forensisch expert [VERTROUWELIJK] heeft geconstateerd dat bij het datalek 57.383.315 Uber gebruikers waren betrokken, waarvan 25.606.182 Amerikaanse en 31.777.133 niet-Amerikaanse.[71] Verder blijkt uit informatie van Uber dat ongeveer 174.000[72] Nederlandse Uber-gebruikers zijn getroffen door het datalek. Over de bij het datalek betrokken persoonsgegevens merkt de AP verder op dat het gaat om - zoals kan worden opgemaakt uit het door [VERTROUWELIJK] uitgevoerde onderzoek - 31 soorten persoonsgegevens, zoals in de paragraaf 'feiten en procesverloop' weergegeven.

De omvang van de bij het datalek betrokken persoonsgegevens, het grote aantal verschillende soorten persoonsgegevens, het type persoonsgegevens (namen, e-mailadressen en telefoonnummers) alsmede het feit dat het persoonsgegevens betreft van klanten van één specifieke – wereldwijd opererende – onderneming, maken de persoonsgegevens extra aantrekkelijk om bijvoorbeeld te worden doorverkocht[73] ten behoeve van activiteiten als '(spear) phishing'[74], ongewenste reclame (spam) en/of ongewilde telefonische colportage.[75]

Afgezien van het feit dát onbevoegden toegang hebben gekregen tot de opslag van Uber en bijgevolg reeds kan worden betoogd dat sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen, als bedoeld in artikel 34a, eerste lid, van de Wbp, is daarvan te meer sprake, althans is daarvan in elk geval sprake gelet op de omvang van de betrokken persoonsgegevens, het type persoonsgegevens en het feit dat deze afkomstig waren van klanten van één onderneming, die bovendien wereldwijd actief is. Dientengevolge was Uber wettelijk verplicht om het datalek te melden. Het betoog van Uber dat van ernstige nadelige gevolgen, althans de aanzienlijke kans daarop geen sprake zou zijn, acht de AP dan ook onjuist.

Louter ter illustratie merkt de AP in dit verband nog het volgende op. Als Uber daadwerkelijk zou menen dat zij het datalek niet had hoeven te melden dan verbaast het de AP dat UTI niettemin heeft besloten om de melders van het datalek te 'belonen' met een bedrag dat substantieel hoger lag dan wat normaal gesproken wordt uitgekeerd, en bij hen geheimhouding van het datalek heeft bedongen.[76] Dit impliceert

[70] Vgl. *Kamerstukken II* 2012/13, 33 662, nr. 3 Herdruk, p. 7.
[71] Rapport [VERTROUWELIJK], p. 7-9.
[72] Vgl. annex 4 bij brief Uber van 1 december 2017 (antwoord vraag 5).
[73] Bijvoorbeeld op de zwarte markt via het 'dark web'.
[74] Phishing is een vorm van internetfraude waarbij iemand valse e-mails ontvangt die hem naar een nagebootste website probeert te lokken. Vgl. https://www.rijksoverheid.nl/onderwerpen/cybercrime/vraag-en-antwoord/phishing. Een vorm van phishing is spear fishing. Hierbij worden de persoonlijke gegevens (naam, e-mailadres, telefoonnummer) van het slachtoffer gebruikt om hem een gevoel van vertrouwen te geven. Er komt een e-mail binnen, die van een betrouwbare bron afkomstig lijkt te zijn, maar in werkelijkheid leidt hij de gebruiker naar een vervalste website, die bijvoorbeeld vol met malware zit. Zo'n gerichte aanval is vaak succesvoller dan een algemene phishingcampagne.
[75] Vgl. paragraaf 4.2.2, p. 27-28 van de beleidsregels *'De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)'* van 8 december 2015 (*Stcrt.* 2015, nr 46128). Zie ook: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-beleidsregels-meldplicht-datalekken
[76] In dit verband wordt verwezen naar hetgeen hierover in onderhavig besluit is overwogen bij de ernstig verwijtbare nalatigheid.

volgens de AP juist dat Uber het datalek kennelijk zelf ook als bijzonder ernstig beschouwt en ook ernstige nadelige gevolgen had voor de bescherming van persoonsgegevens, althans daarop een aanzienlijke kans bestond. De melder van het datalek heeft Uber ook uitdrukkelijk gewezen op de risico's, hoewel hij wellicht ook andere intenties had[77]: "*Let me tell you this looks bad. I suggest you speak with employees on re-using passwords. My team was able to access alot of internal information.* [VERTROUWELIJK]"

De impact en ernst van het datalek en daarmee ondersteunend aan de conclusie van de AP dat sprake is van (de aanzienlijke kans op) ernstige nadelige gevolgen, kan ook worden afgeleid uit het feit dat de [VERTROUWELIJK] van UTI ten overstaan van een subcommissie van de Senaat van de Verenigde Staten. het aan de melders hoger dan normaal uitgekeerde bedrag heeft verdedigd en heeft verklaard dat dit is gedaan met het oog op de bescherming van persoonsgegevens van de klanten van Uber.[78] Bovendien heeft de CEO van Uber publiekelijk ruchtbaarheid gegeven aan het datalek via een mededeling op haar website.[79] Ook is uit verschillende openbare bronnen, waaronder de website van Uber, gebleken dat Uber in verband met het verzwijgen van dit datalek onlangs een schikking ter waarde van 148 miljoen dollar heeft getroffen met de autoriteiten in de Verenigde Staten.[80] Ook tegen die achtergrond volgt de AP Uber niet in haar stelling dat van ernstige gevolgen voor de bescherming van persoonsgegevens, dan wel de aanzienlijke kans daarop, geen sprake zou zijn, en Uber de melding slechts 'onverplicht en uit eigen beweging' en 'in het kader van transparantie' zou zijn gedaan.

Overige onderdelen zienswijze Uber en reactie AP
Dat de onbevoegden deze gegevens - tot op heden - niet verder hebben verspreid, doorverkocht of anderszins hebben verwerkt, betekent volgens de AP niet dat, zoals Uber betoogt in haar zienswijze, daarmee dus geen sprake was van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. De AP verwijst naar hetgeen hiervoor in deze paragraaf is overwogen over de (aanzienlijke kans op) ernstige nadelige gevolgen. Ook de in dit verband door Uber geponeerde stelling in haar zienswijze dat geen sprake is van persoonsgegevens van gevoelige aard, betekent naar het oordeel van de AP niet dat een datalek zoals het onderhavige niet gemeld hoeft te worden. Anders dan Uber meent, kan dat ook niet worden opgemaakt uit de beleidsregels. In de beleidsregels staat: *(...) Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is er over het algemeen een melding noodzakelijk. (...)*.[81]Kortom, het is één van de relevante factoren bij beantwoording van de vraag of een datalek meldingsplichtig is. Dat betekent volgens de AP echter niet dat in het geval er persoonsgegevens zijn gelekt die niet gevoelig zijn, het datalek dus altijd van de meldplicht verschoond zou zijn. Ook andere factoren zoals de hoeveelheid gelekte persoonsgegevens per persoon of

[77] Zie e-mail wisseling op 14, 15 en 16 november 2016 tussen de melder en medewerkers van Uber (bijlage 3 bij de brief van Uber van 11 december 2017 gevoegd).
[78] Zie bijlage bij de brief van Uber van 7 februari 2018.
[79] Vgl. onder 4.26 van de zienswijze Uber, p. 30.
[80] Zie onder meer: https://www.uber.com/newsroom/2016-data-breach-settlement/, https://www.reuters.com/article/us-uber-databreach/uber-settles-for-148-million-with-50-us-states-over-2016-data-breach-idUSKCN1M62AJ, https://nos.nl/artikel/2252243-uber-schikt-voor-148-miljoen-dollar-na-verzwijgen-datalek.html, https://www.iowaattorneygeneral.gov/newsroom/uber-hackers-data-breach-miller-attorneys/ en https://oag.ca.gov/news/press-releases/california-attorney-general-becerra-san-francisco-district-attorney-gasc%C3%B3n
[81] Vgl. Beleidsregels '*Meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)*', p. 2.

het aantal betrokkenen van wie persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Dit blijkt ook uit de beleidsregels.[82] Vorenstaande gaat ook op voor de stelling van Uber in haar zienswijze dat het datalek op 15 november 2016 is verholpen, de onbevoegden uit waren op een beloning en er geen indicatie van misbruik of kans op misbruik van persoonsgegevens was. Ook deze omstandigheden, wat daar verder ook van zij, brengen niet met zich mee dat onderhavig datalek niet meldingsplichtig was.

3.3.5 Datalek niet onverwijld gemeld

Indien sprake is van een meldingsplichtig datalek, verplicht artikel 34a, eerste lid, van de Wbp de verantwoordelijke om de toezichthouder hiervan 'onverwijld' in kennis te stellen. Wat in een concreet geval als 'onverwijld' moet worden aangemerkt, hangt af van de omstandigheden van het geval. Ratio is dat de verantwoordelijke enige tijd moet worden gegund om onderzoek te doen naar de inbreuk. De wetgever heeft het aan de toezichthouder gelaten om het begrip 'onverwijld' nader te duiden.[83] De AP heeft dit gedaan in de meergenoemde beleidsregels *'Meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)'* van 8 december 2015.[84] De melding van het datalek moet - blijkens paragraaf 6 van de beleidsregels - zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, bij de AP worden gedaan. Hoofdregel is dus dat de melding zonder onnodige vertraging moet worden gedaan, waarbij 72 uur in principe geldt als uiterste limiet. In dit verband zij overigens opgemerkt dat ook een voorlopige melding kan worden gedaan.[85] Daarmee zal er in de praktijk niet snel aanleiding zijn om niet binnen de gestelde termijn van 72 uur melding te maken van een datalek.

Zoals eerder weergegeven, worden UTI en UBV door de AP gezien als gezamenlijk verantwoordelijke. Op maandag 14 november 2016 is UTI op de hoogte gesteld van een kwetsbaarheid in haar gegevensbeveiliging. Immers, op die datum ontving de toenmalige [VERTROUWELIJK]van UTI een e-mailbericht van een persoon[86] die de [VERTROUWELIJK] informeerde dat hij een grote kwetsbaarheid in de gegevensbeveiliging van het Uber-concern had ontdekt.[87]Op 15 november 2016 zijn documenten, met daarin de betreffende persoonsgegevens, gedownload en konden die worden ingezien.[88] Zo merkt de onbevoegde in de e-mail correspondentie aan Uber op*"(...) ALL INTERNAL data was able to be downloaded and seen (...)"* en "*(...)*[VERTROUWELIJK] *(...)"*. Op 15 november 2016 heeft de [VERTROUWELIJK] van UTI opdracht gegeven om toegangscodes tot Ubers AWS S3 opslag te wijzigen.[89] Op basis van de informatie over de inbreuk waarover UTI dus op 15 november 2016 al de beschikking had, zag UTI zich genoodzaakt maatregelen te treffen.

---

[82] Idem.
[83] Vgl. *Kamerstukken II* 2013/14, 33 662, nr. 6, p. 16.
[84] *Stcrt.* 2015, 46128, p. 14-15.
[85] Bijvoorbeeld omdat nog niet duidelijk is wat er is gebeurd en om welke persoonsgegevens het gaat. Zo nodig kan de melding dan worden aangevuld of ingetrokken. Vgl. paragraaf 6, p. 31 van de beleidsregels *'Meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp).*
[86] Deze persoon maakte daarbij gebruik van een pseudoniem e-mailadres.
[87] Deze e-mail is als bijlage 3 bij de brief van Uber van 11 december 2017 gevoegd.
[88] Appendix b, tabel 3, p. 11 en 12 van het rapport van [VERTROUWELIJK].
[89] Vgl. e-mailconversatie op 15 november 2016 (meer specifiek de e-mail aan de melder van 15 november 2016 van 9:29 AM), die als bijlage 3 bij de brief van Uber van 11 december 2017 is gevoegd.

De AP is gelet op het vorenstaande van oordeel dat UTI al op 15 november 2016 redelijkerwijs melding had kunnen en moeten maken van het datalek, omdat een melding ná dat moment gelet op de hiervoor genoemde omstandigheden naar het oordeel van de AP kan worden gekwalificeerd als een 'onnodige vertraging' als bedoeld in de beleidsregels. Maar de melding had in elk geval uiterlijk binnen 72 uur na 14 november 2016 - de dag dat Uber op de hoogte is gesteld van het datalek - dienen plaats te vinden. Dit had óók redelijkerwijs moeten gebeuren als op dat moment de precieze omvang van het datalek nog niet bekend was, of nog niet kon worden overzien. Als gezegd, kon immers ook een voorlopige melding worden gedaan.

UBV heeft op 21 november 2017 het datalek aan de AP gemeld middels het daartoe op de website van de AP ter beschikking gestelde webformulier. De termijn voor het melden van het datalek begint blijkens voormelde beleidsregels:

> *"te lopen op het moment dat uzelf, of een bewerker die u heeft ingeschakeld, op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt."*[90]

UTI en UBV zijn gezamenlijk verantwoordelijke en dus op zowel UTI als UBV afzondelijk de plicht rustte om het datalek uiterlijk binnen 72 uur nadat UTI op 14 november 2016 daarvan op de hoogte werd gesteld bij de AP te melden. De melding van het datalek is eerst gedaan op 21 november 2017 en daarmee 371 dagen na de ontdekking ervan, waarmee de voorgeschreven termijn van 72 uur ruimschoots is overschreden. Van een onverwijlde melding als bedoeld in artikel 34a, eerste lid, van de Wbp is derhalve geen sprake. Daarbij merkt de AP wel op dat, nu UBV het datalek op 21 november 2017 aan de AP heeft gemeld, de AP deze melding beschouwt als mede namens UTI gedaan. UTI hoeft de melding daarom niet (nogmaals) te doen.

Los daarvan merkt de AP op dat nu de termijn voor melding op basis van de beleidsregels (mede) wordt bepaald door het tijdstip waarop de bewerker op de hoogte raakt van het incident - en voor zover UTI in deze context als bewerker zou moeten worden aangemerkt - Uber zich niet kan verschuilen achter de omstandigheid dat UTI als bewerker louter haar privaatrechtelijke verplichtingen niet is nagekomen jegens UBV, zoals zij in haar zienswijze naar voren brengt.

Geheel ten overvloede merkt de AP bovendien nog op dat ook in het geval UBV als (enige) verantwoordelijke zou moeten worden aangemerkt, of als UBV zich er – als gezamenlijke verantwoordelijke met UTI – gerechtvaardigd op kan beroepen dat zij eerst op een later moment door UTI van het datalek op de hoogte is gebracht, de melding op 21 november 2017 door UBV aan de AP nog steeds niet 'onverwijld' na kennisname bij UBV is gedaan. UBV is in de persoon van de [VERTROUWELIJK] immers op 25 oktober 2017 op de hoogte geraakt van, wat Uber in haar zienswijze noemt, een "*IT security incident in 2016, that it was being investigated, and that it could potentially create a media cycle.*"[91] Naar het oordeel van de AP kan UBV geen gerechtvaardigd beroep doen op onwetendheid, die eruit bestaat dat de

[90] Vgl. paragraaf 6, p. 31 van de beleidsregels *'De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)'*.
[91] Bijlage 1 bij de schriftelijke zienswijze van Uber van 3 juli 2018.

[VERTROUWELIJK] van UBV geen "*knowledge of the scope of the incident, or if personal data was involved*" had.[92] Met de informatie die op 25 oktober 2017 wél bekend was bij [VERTROUWELIJK] van UBV - een IT veiligheidsincident dat potentiële media- aandacht kan veroorzaken - had het naar het oordeel van de AP redelijkerwijs op zijn weg gelegen om kritisch door te vragen om aldus te achterhalen of er sprake was van een datalek, óf daarbij persoonsgegevens waren betrokken en wat de relevantie van het '*IT security incident*' was voor UBV. En zelfs als er van moet worden uitgaan dat UBV eerst 10 november 2017 voor het eerst in kennis zou zijn gesteld van het datalek, zoals Uber betoogt,[93] dan nog is sprake van een ruime overschrijding van de voorgeschreven termijn van 72 uur en is van een onverwijlde melding evenmin sprake.[94]

Het belang van een onverwijlde melding is, zoals hiervoor al uiteengezet, onder meer gelegen in het behoud en herstel van het vertrouwen van het publiek, de klanten en de toezichthouders in Uber. Een onverwijlde melding stelt de AP in staat zich tijdig een eigen beeld te vormen van de feiten, een oordeel te kunnen geven over de genomen maatregelen en onder omstandigheden vertrouwelijk met de verantwoordelijke kunnen overleggen en zo nodig kunnen interveniëren.[95] Omdat in dit geval de voorgeschreven termijn van 72 uur ruimschoots is overschreden en derhalve van een onverwijlde melding van het datalek geenszins kan worden gesproken, is sprake van een situatie waarin dat vertrouwen in hoge mate is beschaamd. In dit verband wordt nogmaals benadrukt dat een datalek ook onder voorbehoud kan worden gemeld en zo nodig kan worden aangevuld of ingetrokken.

Zienswijze Uber en reactie AP
De door Uber gegeven verklaring voor het niet binnen de termijn van 72 uur melden aan de AP van het datalek is in het onderzoeksrapport aangemerkt als onvoldoende gemotiveerd. Uber heeft aangegeven dat niet tijdig is gemeld, maar dat zij niet kan verklaren waarom dat niet is gebeurd.[96] De stelling van Uber in haar zienswijze waarin zij aangeeft dat UBV nadat zij op de hoogte was gesteld door UTI van het datalek alsnog binnen een 'adequate' termijn op 21 november 2017 het datalek aan de AP heeft gemeld (en via haar gemachtigde op 20 november het voornemen om melding te maken aan de AP kenbaar gemaakt) overtuigt de AP niet. Zoals opgemerkt, had (ook) UTI, als (gezamenlijk) verantwoordelijke op 15 november 2016, althans in elk geval uiterlijk binnen 72 uur nadat UTI op 14 november 2016 van het datalek in kennis werd gesteld, het datalek kunnen en moeten melden.

Uber stelt in haar zienswijze verder nog dat het meldingsformulier niet is gemaakt voor buitenlandse ondernemingen en specifiek gericht is op Nederlandse ondernemingen. Dienaangaande merkt de AP op dat hieruit niet kan worden geconcludeerd dat dit UTI, als gezamenlijk verantwoordelijke, zou ontslaan van haar meldplicht aan de AP dan wel dat dit een beletsel zou zijn om het datalek (onverwijld) te melden. UTI had hierover met AP in contact kunnen treden. Hierbij merkt de AP geheel ten overvloede nog op dat

[92] Idem.
[93] Deze datum staat blijkens paragraaf 5.26, p. 37 van de zienswijze van Uber in elk niet ter discussie als de datum waarop UBV door UTI in kennis is gesteld van het datalek.
[94] Een onverwijlde melding, dus binnen 72 uur en zo nodig voorwaardelijk, had juist dán voor de hand gelegen omdat het datalek zich al in 2016 had voorgedaan.
[95] Vgl. *Kamerstukken II* 2012/13, 33 662, nr. 3 Herdruk, p. 4.
[96] Vgl. paragraaf 5.3.3. p. 38 -39, van het onderzoeksrapport.

de website van de AP ook een Engelse versie kent waarin wordt gewezen op de mogelijkheid met de AP in contact te treden. Bovendien had UTI gebruik kunnen maken van UBV als aanspreekpunt dan wel een gemachtigde in Nederland kunnen aanwijzen.

3.3.6 Conclusie

Uit het vorenstaande concludeert de AP dat UBV en UTI, als (gezamenlijk) verantwoordelijke op 15 november 2016, althans in elk geval binnen uiterlijk 72 uur nadat UTI op 14 november 2016 in kennis was gesteld van het datalek op grond van artikel 34a, eerste lid, van de Wbp verplicht was/waren het datalek te melden aan de AP. De melding aan de AP heeft echter eerst plaatsgevonden op 21 november 2017 en was daarmee niet onverwijld als bedoeld in dat artikellid. Gelet hierop is sprake van een overtreding van artikel 34a, eerste lid, van de Wbp, waarbij UBV en UTI beide overtreder zijn. Voor zover moet worden aangenomen dat – naar de interpretatie van Uber - uitsluitend UBV verantwoordelijke en UTI bewerker is, leidt deze aanname niet tot een andere conclusie, nu de termijn van 72 uur op basis van de beleidsreels loopt met ingang van het moment waarop de bewerker (UTI in dit geval) op de hoogte van het incident, te weten 14 november 2016.

3.4 Overtreding meldplicht aan betrokkene

3.4.1 Inleiding

Zoals uit subparagraaf 2.1.5 blijkt, gold per 1 januari 2016 op grond van artikel 34a, tweede lid, van de Wbp een meldplicht van datalekken aan de betrokkenen. Ingevolge deze meldplicht moet de verantwoordelijke de betrokkene onverwijld in kennis stellen van een inbreuk op de beveiliging als de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Zowel UBV als UTI is, als gezamenlijk verantwoordelijke, hiervan normadressaat. De AP verwijst in dit verband kortheidshalve naar hetgeen in hierboven reeds is overwogen over de overtreding van de meldplicht aan de AP. Hetzelfde geldt ten aanzien van de inbreuk op de beveiliging.

3.4.2 Inbreuk zal waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer

Ingevolge artikel 34a, tweede lid, van de Wbp is sprake van een meldplichtige inbreuk als de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van betrokkene(n) die het aangaat. Omdat in dit geval onbevoegden bestanden van Uber van haar AWS S3 opslag hebben gedownload en daarmee toegang hadden tot, en kennis konden nemen van, de daarin opgenomen persoonsgegevens van Uber klanten is naar het oordeel van de AP sprake van ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkenen wiens persoonsgegevens het betrof. De AP merkt ten aanzien van de reikwijdte van het begrip persoonlijke levenssfeer nog op, dat persoonsgegevens worden beschermd als een onderdeel van de persoonlijke levenssfeer in de zin van artikel 10 van de Grondwet en als onderdeel van het recht op respect voor privéleven in de zin van artikel 8 van het EVRM.[97] Een ieder heeft er recht op dat zijn persoonsgegevens op een rechtmatige wijze worden verwerkt, om te voorkomen dat hij hier nadeel van ondervindt.

[97] Kamerstukken 2017/18, 34 851, nr. 3, p. 7.

Naast het feit dát onbevoegden toegang hadden tot de opslag van Uber – en daarmee tot de daarin opgeslagen persoonsgegevens van Uber klanten – maakt de omvang van de bij het datalek betrokken persoonsgegevens[98], het type persoonsgegevens (namen, e-mailadressen en telefoonnummers) alsmede het feit dat het persoonsgegevens betreft van klanten van één specifieke - wereldwijd opererende - onderneming dat te meer sprake is van (waarschijnlijk) ongunstige gevolgen. Door deze combinatie van factoren wordt de dataset extra aantrekkelijk om bijvoorbeeld te worden doorverkocht[99] ten behoeve van activiteiten als (spear) phishing[100], ongewenste reclame (spam) en/of ongewilde telefonische colportage.

Toen halverwege november 2016 Uber op de hoogte raakte van het datalek en de persoonsgegevens die daarbij waren betrokken, was er voldoende aanleiding om een melding te doen aan betrokkenen vanwege te duchten ongunstige gevolgen, zoals het risico op bijvoorbeeld (spear)phising. Op dat moment was het een reëel risico en kon dat redelijkerwijs niet worden uitgesloten.

Op basis van het vorenstaande concludeert de AP dat Uber in dit geval op grond van artikel 34a, tweede lid, Wbp, verplicht was om het datalek te melden aan de betrokkenen die het aanging. In dit verband merkt de AP overigens nog op dat gesteld noch gebleken is dat zich een situatie voordoet als bedoeld in artikel 43 Wbp en op grond waarvan de verantwoordelijke de meldplicht uit artikel 34a, tweede lid, Wbp buiten toepassing kan laten.

3.4.3 Datalek niet (onverwijld) gemeld

De AP stelt vast dat het datalek niet is gemeld aan de betrokkenen en daarmee evenmin sprake was van een onverwijlde melding, zoals artikel 34a, tweede lid, van de Wbp dat vereist. Wat in een concreet geval als onverwijld moet worden aangemerkt, hangt af van de omstandigheden van het geval. In de meermaals genoemde beleidsregels over datalekken geeft de AP aan dat het onverwijld melden betekent, dat na het ontdekken van het datalek, enige tijd mag worden genomen voor nader onderzoek zodat de betrokkenen op een behoorlijke en zorgvuldige manier kunnen worden geïnformeerd door de verantwoordelijke. Uit de beleidsregels blijkt verder dat, net als bij de melding aan de AP, ervoor kan worden gekozen om de betrokkenen in eerste instantie te informeren op basis van de informatie waarover op dat moment wordt beschikt, zodat de betrokkenen alvast maatregelen kunnen treffen. Een maatregel kan al inhouden dat betrokkenen extra bedachtzaam zijn. Later kan de informatie zo nodig dan nog worden aangevuld.[101] Tegen deze achtergrond, en onder verwijzing naar hetgeen hierover in dit besluit is opgemerkt bij de overtreding van de meldplicht aan de AP, wordt opgemerkt dat Uber op 14 november 2016 van het datalek op de hoogte is gesteld. De AP is van mening dat Uber gerekend van 14 november 2016 uiterlijk binnen 72 uur, en in lijn

[98] Hiervoor in dit besluit bij de overtreding van de meldplicht aan de AP is al aangegeven dat het gaat om gegevens van 57.383.315 Uber gebruikers, waarvan 25.606.182 Amerikaanse en 31.777.133 niet-Amerikaanse. Waar het betreft de Nederlandse Uber-gebruikers gaat om ongeveer 174.000 getroffenen.
[99] Bijvoorbeeld op de zwarte markt via het 'dark web'.
[100] Phishing is een vorm van internetfraude waarbij iemand valse e-mails ontvangt die hem naar een nagebootste website probeert te lokken. Vgl. https://www.rijksoverheid.nl/onderwerpen/cybercrime/vraag-en-antwoord/phishing. Een vorm van phishing is spear phishing. Hierbij worden de persoonlijke gegevens (naam, e-mailadres, telefoonnummer) van het slachtoffer gebruikt om hem een gevoel van vertrouwen te geven. Er komt een e-mail binnen, die van een betrouwbare bron afkomstig lijkt te zijn, maar in werkelijkheid leidt hij de gebruiker naar een vervalste website, die bijvoorbeeld vol met malware zit. Een dergelijk gerichte aanval is vaak succesvoller dan een algemene phishingcampagne.
[101] Zie p. 45 van de beleidsregels over datalekken.

met hetgeen de AP heeft overwogen ten aanzien van de meldplicht aan de AP, de betrokkenen in kennis had moeten en kunnen stellen van het datalek. Dat is niet gebeurd.

3.4.4 Hoe moet het datalek aan betrokkenen worden gemeld?

Op grond van artikel 34a, vijfde lid, van de Wbp wordt de kennisgeving aan de betrokkene op zodanige wijze gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.

Het melden van een datalek aan betrokkenen dient - zo volgt uit de beleidsregels over datalekken en de wetgeschiedenis[102] - op individuele basis te gebeuren, zoals in een persoonlijke e-mail. In veruit de meeste gevallen zal de verantwoordelijke over contactgegevens van de betrokkenen beschikken en kunnen betrokkenen ook individueel worden geïnformeerd. Bij meer omvangrijke incidenten kan ook een combinatie van algemene en individuele informatievoorziening geschikt zijn, zoals een mededeling op de website van het bedrijf en een individuele e-mail aan getroffen klanten. Het belangrijkste is, dat zoveel mogelijk betrokkenen worden bereikt en geïnformeerd over de door hem of haar zelf te treffen maatregelen om de gevolgen voor de persoonlijke levenssfeer zoveel mogelijk te beperken. Met enkel een bericht in de media wordt dat doel niet bereikt.[103] Naar het oordeel van de AP was het, gelet op de voor Uber beschikbare contactgegevens goed mogelijk de getroffen Uber klanten individueel te benaderen en was alleen een melding in een persbericht niet afdoende.

3.4.5 Zienswijze Uber en reactie AP

Uber stelt in haar zienswijze dat het datalek niet aan betrokkenen hoefde te worden gemeld omdat er verschillende technische en organisatorische beveiligingsmaatregelen zijn getroffen. Dienaangaande merkt de AP op dat de door Uber getroffen beveiligingsmaatregelen erop waren gericht het datalek te dichten en herhaling te voorkomen. Dit betekent echter niet dat hieruit geconcludeerd moet worden dat gedurende de periode van de inbreuk er geen sprake was van een situatie dat de inbreuk waarschijnlijk ongunstige gevolgen zal hebben. Zoals hiervoor uiteengezet, is de AP van mening dat er wel sprake van een inbreuk die waarschijnlijk ongunstige gevolgen zal hebben. Ook rechtvaardigen de door Uber getroffen maatregelen geen beroep op artikel 34a, zesde lid, van de Wbp op grond waarvan een melding aan betrokkene achterwege kan blijven. Veel persoonsgegevens - waaronder namen, e-mailadressen en telefoonnummers - waren ten tijde van het lek immers onbeschermd (onversleuteld) en toegankelijk voor en in het bezit van onbevoegden. De maatregelen waaraan Uber refereert, werden als gezegd nadien getroffen om het lek te dichten en herhaling te voorkomen.

Uber geeft verder aan dat het niet waarschijnlijk was dat het datalek ongunstige gevolgen zou hebben omdat het niet gaat om gevoelige gegevens.

[102] Vgl. p. 43 van de beleidsregels over datalekken en Kamerstukken I, 2014/15, 33 662, nr. C, p. 15.
[103] Kamerstukken I, 2014/15, 33 662, nr. C, p. 15.

In het geval er persoonsgegevens van gevoelige aard zijn gelekt moet ervan uit worden gegaan dat het datalek niet alleen aan de AP, maar ook aan de betrokkenen moet worden gemeld.[104] Het is met andere woorden een zeer belangrijke indicatie dat een melding aan betrokkenen moet worden gedaan. Op grond van de beleidsregels blijkt dat in alle overige gevallen de verantwoordelijke op basis van de omstandigheden van het geval een afweging zal moeten maken. De omstandigheid dat een datalek niet ziet op gevoelige gegevens, betekent dan ook niet dat een melding aan betrokkenen dus achterwege kan blijven. In dit geval waren er voldoende redenen op grond waarvan Uber gehouden was het datalek aan betrokkenen te melden.

Uber betoogt in haar zienswijze verder dat er geen bewijs is dat meer dan twee individuen gedurende een korte periode toegang hadden tot de betreffende persoonsgegevens, dat Uber inloggegevens onbruikbaar heeft gemaakt en tweefactor authenticatie heeft ingevoerd. Volgens Uber duidt alles erop dat de onbevoegden de gedownloade bestanden hebben verwijderd zonder deze te delen met anderen. Uber heeft geheimhoudingsovereenkomsten met de onbevoegden getekend en kent hun identiteit. Dat bepaalde persoonsgegevens voor korte duur beschikbaar waren voor twee individuen maakt het volgens Uber niet waarschijnlijk dat de bewuste persoonsgegevens (namen, e-mailadressen, telefoonnummers) voor spam of phising worden gebruikt, nog afgezien van de vraag of dit kan worden gezien als een inbreuk op de persoonlijke levenssfeer.

De AP volgt Uber niet in haar betoog. Dat er aanwijzingen zijn dat de onbevoegden de bestanden hebben verwijderd, zij een geheimhoudingsverklaring hebben getekend en hun identiteit hebben prijsgegeven, en het volgens Uber niet waarschijnlijk is dat de bewuste persoonsgegevens voor spam of phising zijn gebruikt, neemt niet weg dát de persoonsgegevens toegankelijk waren voor onbevoegden en dat dit, zoals eerder overwogen, gelet op de omvang en het type persoonsgegevens en het feit dat het ging om klanten van één onderneming een aanmerkelijk risico van verdere verspreiding inhield. Overigens valt ook op dit moment niet uit te sluiten dat de bewuste gegevens niet toch nog ergens - buiten Uber om - beschikbaar zijn. Het datalek heeft gedurende vijf weken bestaan. Gedurende die periode hadden de onbevoegden toegang tot de betreffende persoonsgegevens zonder dat Uber daar invloed op had. Dat heeft, zoals hiervoor uiteengezet, risico's met zich meegebracht. Daarmee was er naar het oordeel van de AP voldoende reden om te concluderen dat het datalek op grond van artikel 34a, tweede lid, Wbp gemeld had moeten worden aan de betrokkenen.

In haar zienswijze stelt Uber tot slot dat zij uit het tijdsverloop en het ontbreken van enige aanwijzing van de AP omtrent melding aan betrokkenen - de AP heeft sinds de melding van het datalek aan de AP in november 2017 Uber niet verplicht om het datalek aan betrokkene te melden - heeft mogen openmaken dat ook de AP vindt dat het onwaarschijnlijk is dat het datalek ongunstige gevolgen kon hebben voor de betrokkenen.

De AP volgt Uber niet in haar betoog. De AP merkt daartoe allereerst op dat het aan UTI en UBV als verantwoordelijke is om te beoordelen of een datalek gemeld moet worden aan betrokkenen en niet aan de

[104] Vgl. p. 39 van de beleidsregels over datalekken.

AP.[105] Die beoordeling moet worden gemaakt op het moment dat het datalek aan Uber bekend was. Dat was al op 14 november 2016. Zoals hiervoor gemotiveerd uiteengezet was er toen voldoende reden om aan betrokkenen melding van het datalek te doen. Dat achteraf bezien er tot op heden nog niet is gebleken van ongunstige gevolgen als gevolg van bijvoorbeeld phising activiteiten, maakt dat naar het oordeel van de AP niet anders. De beoordeling of het datalek ernstige gevolgen heeft of zal hebben voor de bescherming van persoonsgegevens dient namelijk gemaakt te worden op het moment van het datalek.

3.4.6 Conclusie

Uit het vorenstaande concludeert de AP dat UBV en UTI, als gezamenlijk verantwoordelijke betrokkenen ten onrechte en in strijd met artikel 34a, tweede lid, van de Wbp niet onverwijld in kennis hebben gesteld van het datalek. Derhalve is sprake van een overtreding van 34a, tweede lid, van de Wbp, waarbij UBV en UTI beide overtreder zijn.

3.5 Ernstig verwijtbare nalatigheid

3.5.1 Inleiding

Hiervoor heeft de AP geconcludeerd dat UBV en UTI gezamenlijk verantwoordelijke zijn in de zin van artikel 1, aanhef, en onder d, van de Wbp, als gevolg waarvan UBV en UTI beide normadressaat van de verplichting ex artikel 34a, eerste en tweede lid, van de Wbp zijn. Het achterwege blijven van een tijdige melding van het datalek aan de AP en het tijdig in kennis stellen van betrokkenen is naar het oordeel van de AP het gevolg van ernstig verwijtbare nalatigheid. Hierna motiveert de AP dat standpunt. Daartoe zal zij allereerst het wettelijk kader uiteenzetten en schetsen welke kennis een normadressaat daarvan geacht wordt te hebben. Vervolgens zal de AP de wetenschap van het Uber-concern over de ernst van het datalek beoordelen. Daarna zal de AP feiten en omstandigheden duiden die naar het oordeel van de AP maken dat het achterwege blijven van een tijdige melding van het datalek aan de AP en het tijdig in kennis stellen van betrokkenen het gevolg is van ernstig verwijtbare nalatigheid.

3.5.2 Wettelijk kader

Artikel 66, derde en vierde lid, van de Wbp luidde ten tijde van de overtreding, voor zover van belang, als volgt:

> *"(...)*
> 3. *Het College legt geen bestuurlijke boete op wegens overtreding van het bepaalde bij of krachtens de in artikel 66, tweede lid, genoemde artikelen, dan nadat het een bindende aanwijzing heeft gegeven. Het College kan de overtreder een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd.*
> 4. *Het derde lid is niet van toepassing indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid.*
>
> *(...)"*

Blijkens de parlementaire geschiedenis is van 'ernstig verwijtbare nalatigheid' als bedoeld in artikel 66, vierde lid, van de Wbp sprake indien "*de overtreding het gevolg is van ernstig verwijtbare nalatigheid, dat wil zeggen*

[105] Vgl. p. 39 van de beleidsregels over datalekken

het gevolg is van grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen."[106] In dit verband wordt opgemerkt dat onder "*handelen*" als hiervoor bedoeld, ook een nalaten wordt verstaan.[107]

Zowel in de parlementaire geschiedenis als in de Beleidsregels meldplicht datalekken uit 2015 worden voorbeelden van datalekken genoemd die moeten worden gemeld aan de AP. Ter illustratie worden onder meer genoemd:

- een bedrijf krijgt te maken met een hack waarbij klantgegevens en wachtwoorden zijn ontvreemd;
- op de website van een telefoonbedrijf kunnen klanten inloggen en hun financiële gegevens en belgegevens inzien. Een derde partij heeft toegang gekregen tot de database met inlognamen en bijbehorende verhaspelde (onleesbaar gemaakte) wachtwoorden. Het is echter mogelijk dat bepaalde wachtwoorden achterhaald kunnen worden. [108]

In de Beleidsregels meldplicht datalekken wordt voorts ingegaan op de vraag wanneer een datalek moet worden gemeld aan de AP. Volgens artikel 34a, eerste lid, van de Wbp dient dit "*onverwijld*" te geschieden. In de Beleidsregels meldplicht datalekken heeft de AP het begrip "*onverwijld*" gepreciseerd. Volledigheidshalve citeert de AP de betreffende passage integraal.

> "***6. Wanneer moet ik het datalek melden aan de Autoriteit Persoonsgegevens?***
> *U moet het datalek onverwijld melden aan de Autoriteit Persoonsgegevens (artikel 34a, eerste lid, Wbp).*
>
> *Het onverwijld melden houdt in dat u, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen.*
>
> *Wat in een concreet geval als 'onverwijld' moet worden aangemerkt zal afhangen van de omstandigheden van het geval. Onderstaand treft u de uitgangspunten aan die de Autoriteit Persoonsgegevens met het oog op zijn toezichthoudende en handhavende bevoegdheden hanteert.*
>
> *De termijn voor het melden van het datalek begint te lopen op het moment dat uzelf, of een bewerker die u heeft ingeschakeld, op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt.*
>
> *Zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, doet u een melding bij de Autoriteit Persoonsgegevens, tenzij op dat moment inmiddels al uit uw onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt. Indien u het incident later dan 72 uur na ontdekking aan de toezichthouder meldt, dan kunt u desgevraagd motiveren waarom u de melding later heeft gedaan.*
>
> *Mogelijk heeft u 72 uur na de ontdekking van het incident nog niet volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval doet u de melding op basis van de gegevens waarover u op dat moment beschikt. Eventueel kunt u de melding naderhand nog aanvullen of intrekken.*

[106] *Kamerstukken II* 2014/15, 33662, nr. 16, p. 1.
[107] *Handelingen II* 2014/15, 51, item 9, p. 11.
[108] *Kamerstukken II* 2014/15, 33662, nr. 11, p. 11, *Kamerstukken I* 2014/15, 33662, nr. C, p. 24 en Beleidsregels meldplicht datalekken, *Stcrt.* 2015, 46128, p. 14-15.

Om datalekken tijdig te kunnen melden zult u goede afspraken moeten maken met de bewerkers die u eventueel inschakelt, zodat zij u tijdig en adequaat informeren over alle relevante incidenten."

De AP stelt zich ten aanzien van de kennis die een normadressaat (UBV en UTI gezamenlijk) 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.[109]
De AP heeft marktpartijen ook ruimschoots voorgelicht over de toepasselijke wet- en regelgeving, zodat verondersteld mag worden dat ook Uber 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 toelichting en de Beleidsregels meldplicht datalekken, waar Uber reeds voor het datalek kennis van had kunnen nemen, volgt naar het oordeel van de AP voldoende duidelijk dát Uber het datalek aan zowel de betrokkenen als de AP had moeten melden en dat dit onverwijld, maar in elk geval uiterlijk binnen 72 uur na de ontdekking op 14 november 2016 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 beleidsregel 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 Uber 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.[110]

3.5.3 Wetenschap van het Uber-concern over (de ernst van) het datalek

Naar het oordeel van de AP was het management van UTI zich bewust van de ernst van het datalek. Zulks blijkt ten eerste uit de snelheid waarmee UTI akkoord is gegaan met betaling van een bedrag aan de melders van het datalek. Voorts is het aan de melders betaalde bedrag substantieel hoger dan gebruikelijk. Daarnaast blijkt dit uit de, anders dan normaal te doen gebruikelijke, aanvullende overeenkomsten die met de melders zijn gesloten met de intentie om het datalek geheim te houden. De AP licht dit als volgt toe.

3.5.3.1 Snelheid akkoord betaling

Op maandag 14 november 2016 is UTI op de hoogte gesteld van een kwetsbaarheid in haar gegevensbeveiliging. Immers, op die datum ontving de toenmalige [VERTROUWELIJK]van UTI een e-mailbericht van een persoon die de [VERTROUWELIJK] informeerde dat hij een grote kwetsbaarheid in de gegevensbeveiliging van het Uber-concern had ontdekt.[111] De melder heeft op diezelfde dag aan UTI kenbaar gemaakt dat hij en zijn team een "*high compensation*" voor het signaleren van het datalek aan UTI verwachten.

[109] 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.
[110] 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.
[111] Deze e-mail is als bijlage 3 bij de brief van Uber van 11 december 2017 gevoegd.

Op dinsdag 15 november 2016 laat de melder aan de [VERTROUWELIJK], die het contact met de melder onderhield, weten: "*I am happy that you guys finally found the issue, it was the aws keys that have been leaked, ALL INTERNAL data was able to be downloaded and seen, your security steps are very poorly done, the lack of negligence and care here is zero to none. Your employees are careless and don't care about security. Me and my team found that your team lacks 2 step authenticator on github.*"

De [VERTROUWELIJK] heeft op 15 november 2016 gevraagd naar de ernst van het datalek: "*I'm trying to get some idea on payout amount - can you provide a full list of things you were able to access? That will help me understand impact and then I can pitch an award amount to management.*"
In reactie daarop laat de melder weten: "*Let me tell you this looks bad. I suggest you speak with employees on re-using passwords. My team was able to access alot of internal information.* [VERTROUWELIJK]."

Reeds op vrijdag 18 en maandag 21 november 2016 zijn overeenkomsten getekend door de [VERTROUWELIJK] van UTI en twee individuen. Deze overeenkomsten regelen de betaling van – in totaal – $100.000 voor het melden van het datalek aan UTI.[112]

De [VERTROUWELIJK] van UTI heeft op dinsdag 22 november 2016 een kopie van de overeenkomst met de melders doorgestuurd gekregen.[113] De medewerker van UTI heeft desgevraagd aan de melders bevestigd dat de uitbetaling van de bug bounty in bitcoin gedaan kon worden.[114]

Op vrijdag 9 december 2016 is een bedrag van 65.508 BTC verstuurd naar het bitcoinadres van de melder, die dezelfde dag bevestigde dat hij de bitcoins had ontvangen.[115] Op donderdag 15 december 2016 is nog eens een bedrag van 64.02 BTC verstuurd naar hetzelfde adres.

Uit e-mailwisselingen blijkt ook dat de [VERTROUWELIJK]van UTI op 23 december 2016 op de hoogte was gesteld van de voortgang van maatregelen die zijn genomen naar aanleiding van het datalek.[116]

3.5.3.2 Bovengemiddeld hoge beloning

UTI heeft de melders een beloning van $100.000 betaald voor het melden van het datalek. Dit bedrag is betaald via het bug bounty programma van Hacker One. Dit is een substantieel hoger bedrag dan normaal voor het melden van een kwetsbaarheid wordt betaald door het Uber-concern. Anders dan Uber stelt in haar zienswijze, is dit naar het oordeel van de AP evenzeer een sterke indicatie dat UTI zich bewust was van de ernst van het datalek. Een andersluidende verklaring voor het betalen van een aanzienlijk hoger bedrag dan normaal heeft Uber niet gegeven. Ondanks dat de betaling werd uitgevoerd via HackerOne, heeft Uber kenbaar gemaakt dat de betaling niet is gedaan als onderdeel van het normale Bug Bounty-

[112] Bijlage 3 bij de brief van Uber van 11 december 2017, alsmede de bijlage bij de aanvullende schriftelijke reactie van Uber van 21 februari 2018.
[113] Deze e-mail is als bijlage bij de brief van Uber van 21 februari 2018 gevoegd.
[114] Het verzoek en de bevestiging zijn als bijlage 3 bij de brief van Uber van 11 december 2017 gevoegd.
[115] Zie de e-mail die als bijlage 3 bij de brief van Uber van 11 december 2017 is gevoegd.
[116] Deze e-mail is als bijlage bij de brief van Uber van 21 februari 2018 gevoegd.

programma van Uber.[117] Naar het oordeel van de AP heeft Uber deze melding dan ook bewust anders behandeld dan andere meldingen van kwetsbaarheden.

Op de HackerOne pagina van het Uber-concern staat dat de hoogste bug bounty zich in een bandbreedte tot maximaal $20.000 bevindt. Ten tijde van het datalek gold een typisch maximum van $10.000.[118] De melders hebben te kennen gegeven een "*6 digits*" bug bounty te willen voor het delen van het gevonden lek.[119] Hoewel de uitgekeerde bug bounty van $100.000, betaald via HackerOne in tranches van $10.000, hoger ligt dan het uiterste van de aangegeven bandbreedte verklaart Uber dat de hoogte van uit te keren bug bounties aan de discretie van het Uber-concern is onderworpen.
Op 6 februari 2018 heeft de [VERTROUWELIJK] van UTI tijdens een hoorzitting van een subcommissie van de Senaat van de Verenigde Staten. verklaard dat de betaling het karakter van 'losgeld' voor het verwijderen van de gelekte data had*: "Our primary goal in paying the intruders was to protect our consumers' data."*
Ook verklaart hij*: "We recognize that the bug bounty program is not an appropriate vehicle for dealing with intruders who seek to extort funds from the company. The approach that these intruders took was separate and distinct from those of the researchers in the security community for whom bug bounty programs are designed. While the use of the bug bounty program assisted in the effort to gain attribution and, ultimately, assurances that our users' data were secure, at the end of the day, these intruders were fundamentally different from legitimate bug bounty recipients."*[120]

Uit de snelheid waarmee akkoord werd gegaan met de betaling van bedrag van $100.000, dat een substantieel hoger bedrag is dan gebruikelijk, en de latere verklaring van de [VERTROUWELIJK], blijkt naar het oordeel van de AP dat het management van UTI zich van de ernst van het datalek bewust was ten tijde van die besluitvorming, en zich daarom genoodzaakt voelde om de melders het door hen gevraagde bedrag te betalen om zo verdere schade voor Uber-gebruikers te voorkomen.

3.5.3.3 Geheimhouding

Dat het management van UTI zich bewust was van de ernst van het datalek ten tijde van de besluitvorming in verband met de afhandeling van het gemelde datalek blijkt naar het oordeel van de AP ook uit de aanvullende overeenkomsten die met de melders zijn gesloten met de intentie om het datalek geheim te houden, althans met de bedoeling om openbaarheid te voorkomen.

Geheimhoudingsverplichtingen en verplichtingen om onderzoeksgegevens te verwijderen en niet verder te verspreiden zijn niet ongebruikelijk bij het melden van kwetsbaarheden aan organisaties en bedrijven, ook wel '*responsible disclosure*' geheten. Niet alle bug bounty programma's verplichten echter tot complete geheimhouding van het onderzoek, sommige organisaties maken de bevindingen van de onderzoekers openbaar.

Ten tijde van het datalek was het beleid van het Uber-concern in haar HackerOne bug bounty programma dat onderzoekers over de door hen ontdekte kwetsbaarheden mochten publiceren nadat de kwetsbaarheid

[117] Schriftelijke reactie van Uber van 12 januari 2018 op vragen AP, vraag 29.
[118] Idem.
[119] Deze e-mail is als bijlage bij de brief van Uber van 22 december 2017 gevoegd.
[120] Zie bijlage bij de brief van Uber van 7 februari 2018.

was opgelost door het Uber-concern. Sommige van de door het Uber-concern via HackerOne verholpen kwetsbaarheden zijn door het Uber-concern zelf gepubliceerd. Het Uber-concern heeft via een blogpost informatie gegeven over de eerste honderd dagen van haar bug bounty programma. In die blogpost wordt ook een aantal kwetsbaarheden die via het bug bounty programma zijn opgelost uitgelicht.[121]

In het onderhavige geval heeft UTI echter aanvullende overeenkomsten met de melders gesloten, die het de melders verbood om op wat voor manier dan ook naar buiten te treden met het door hen ontdekte datalek. Deze aanvullende overeenkomst vulde het beleid van het Uber-concern voor HackerOne aan, en regelde de overeenkomst tussen de melders en UTI uitputtend daar waar conflicten tussen het standaard beleid van het Uber-concern en de overeenkomst in kwestie bestonden. Een bepaling omtrent geheimhouding is opgenomen in de overeenkomst waarin de betaling van de bug bounty is geregeld. In deze overeenkomst is bepaald dat *"[researchers] have not and will not disclose anything about the vulnerabilities or your dialogue with us to anyone for any purpose without [UTI's.] written permission. This includes any analysis or post-mortem in any medium or forum."*
De overeenkomst bepaalt verder: *"[Researchers] and [UTI[promise that if [researchers] break [researchers'] promises to [UTI]. [researchers] will repay to [UTI] the bounty reward.]"*[122]

Uit verdere interne communicatie van personeel van UTI blijkt dat geheimhouding van het datalek door de melders essentieel wordt geacht door UTI. In commentaar op een document over de afhandeling van het datalek wordt het volgende geschreven: "*ensuring that the research isn't written about, presented on, etc.*"[123]

Op basis van het bovenstaande stelt de AP vast dat het management van UTI zich bewust was van de ernst van het datalek en het haar er alles aan gelegen was om het datalek geheim te houden, althans om openbaarheid te voorkomen.

3.5.4 Ernstig verwijtbare nalatigheid

Als gezamenlijk verantwoordelijke waren zowel UTI als UBV aansprakelijk voor het geheel van de gegevensverwerking en de daarmee samenhangende verplichtingen. Op zowel UBV als UTI rustte daarmee op grond van artikel 34a, eerste en tweede lid, Wbp de plicht onverwijld melding te doen van het datalek aan zowel de AP als betrokkenen.

UBV en UTI hebben, als gezamenlijk verantwoordelijke, ernstig verwijtbaar nalatig gehandeld door het datalek niet onverwijld te melden aan de AP en betrokkenen. Dat UBV en UTI hebben nagelaten het datalek tijdig bij de AP te melden en betrokken van het datalek tijdig in kennis te stellen is het gevolg van grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen. De AP wijst in dit verband op de volgende feiten en/of omstandigheden in onderling verband beschouwd.

Ten eerste was, zoals hierboven beschreven, het management van UTI reeds op 14 november 2016 op de hoogte van het datalek. Op die datum ontving de toenmalige [VERTROUWELIJK] van UTI een e-

[121] URL: https://eng.uber.com/bug-bounty-update/ (laatst bezocht op 10 oktober 2018).
[122] De overeenkomst is als bijlage 3 bij de brief van Uber van 11 december 2017 gevoegd.
[123] Dit citaat volgt uit een e-mail die als bijlage bij de brief van Uber van 10 januari 2018 is gevoegd.

mailbericht van een persoon die de [VERTROUWELIJK] informeerde dat hij een grote kwetsbaarheid in de gegevensbeveiliging van het Uber-concern had ontdekt.

Ten tweede was het management van UTI zich, zoals hierboven beschreven, vrijwel direct, althans kort na de aanvankelijke melding bewust van de omstandigheden waaruit redelijkerwijs volgt dat sprake is van een inbeuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Ten derde geldt, zoals hierboven beschreven, dat van een groot multinationaal opererende onderneming zoals het Uber-concern mag worden verwacht dat zij zich van de voor haar geldende wettelijke verplichtingen in de landen waarin zij opereert vergewist. De AP gaat er vanuit dat UTI ervan op de hoogte was dat de meldplicht datalekken, zoals geregeld in artikel 34a Wbp, voor haar gold ten tijde van het datalek. Minst genomen had UTI van de verplichting moeten weten.

Onder verwijzing naar het onderdeel overtreding uit dit besluit is de AP van oordeel dat UTI al op 14 november 2016, althans niet later dan 72 uur na de ontdekking op 14 november 2016, het datalek aan de AP had moeten melden.

Ondanks de wetenschap van het datalek, de ernst van het datalek en de duidelijkheid van de toepasselijke wetgeving halverwege november 2016, was het Uber-concern er kennelijk alles aan gelegen om het datalek geheim te houden, althans om openbaarheid te voorkomen en is het datalek pas ruim een jaar na ontdekking van het datalek bij UTI op 21 november 2017 door UBV gemeld aan de AP. In het licht van het vorenstaande kan de AP niet anders concluderen dan dat sprake is van ernstig verwijtbare nalatigheid aan de zijde van UBV en UTI als gezamenlijk verantwoordelijke.

Zelfs als Uber zou moeten worden gevolgd in haar betoog dat enkel UBV als verantwoordelijke dient te worden aangemerkt en UTI als bewerker, dan heeft volgens de Beleidsregels meldplicht datalekken nog steeds te gelden dat het datalek op 14 november 2016, althans niet later dan 72 uur na de ontdekking op 14 november 2016, aan de AP gemeld had moeten worden. In de Beleidsregels meldplicht datalekken is in dit verband opgenomen dat: "*De termijn voor het melden van het datalek begint te lopen op het moment dat uzelf, of een bewerker die u heeft ingeschakeld, op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt.*"

De zienswijze van UBV, dat op 4 november 2017 een eerste bespreking heeft plaatsgevonden tussen UTI en UBV en dat UBV op 10 november 2017 voor het eerst kennis heeft genomen het feit dat het bij de gedownloade bestanden (ook) ging om persoonsgegevens van Nederlandse gebruikers, doet evenmin aan het bovenstaande oordeel van de AP af.
UTI was op grond van de bewerkersovereenkomst gesloten tussen UTI en UBV op 31 maart 2016, verplicht *"[to] promptly notify Uber B.V. about: (ii) any accidental or unauthorised access."*[124] Gezien de gezamenlijk verantwoordelijkheid, de concernverhouding en Beleidsregels meldplicht datalekken kan UBV zich naar het oordeel van de AP niet disculperen met het feit dat UTI heeft nagelaten UBV te informeren.

[124] Annex 1, *Data Processing Agreement,* bij de schriftelijke reactie van Uber van 1 december 2017.

Overigens stelt de AP vast dat de [VERTROUWELIJK] van UBV op 25 oktober 2017 op de hoogte is geraakt van, wat Uber in haar zienswijze noemt, een "*IT security incident in 2016, that it was being investigated, and that it could potentially create a media cycle.*"[125] Naar het oordeel van de AP kan UBV geen gerechtvaardigd beroep doen op onwetendheid, die eruit bestaat dat de [VERTROUWELIJK] van UBV geen "*knowledge of the scope of the incident, or if personal data was involved*" had[126]. Met de informatie die op 25 oktober 2017 wél bekend was bij de [VERTROUWELIJK] van UBV – een IT veiligheidsincident dat potentiële media-aandacht kan veroorzaken - had het naar het oordeel van de AP redelijkerwijs op zijn weg gelegen om kritisch door te vragen om aldus te achterhalen of er sprake was van een datalek, óf daarbij persoonsgegevens waren betrokken en wat de relevantie van het '*IT security incident*' was voor UBV. Door zulks na te laten heeft UBV evenzeer ernstig verwijtbaar nalatig gehandeld.
Zelfs in het geval de AP mee zou gaan in de zienswijze van UBV, namelijk dat zij op 10 november 2017 voor het eerst kennis heeft genomen van de gedownloade bestanden met persoonsgegevens van Nederlandse gebruikers en zij bijgevolg niet later dan 72 uur na die kennisname bij de AP had moeten melden, stelt de AP vast dat UBV met haar melding op 21 november 2017 het datalek ruimschoots te laat heeft gemeld. Evenzeer stelt de AP vast dat UTI en UBV ten onrechte hebben nagelaten betrokkenen onverwijld op de daarvoor voorgeschreven wijze in kennis te stellen van het datalek.

De AP ziet in de overige door Uber in de zienswijze aangedragen omstandigheden geen aanleiding voor een ander oordeel. Niet later dan 72 uur na de ontdekking van het datalek op 14 november 2016 had het datalek aan de AP gemeld moeten worden en hadden betrokkenen van het datalek in kennis moeten worden gesteld.

3.5.5 Conclusie
Naar het oordeel van de AP blijkt uit al het bovenstaande dat UTI en UBV grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig hebben gehandeld, waardoor sprake is van ernstige verwijtbare nalatigheid aan de zijde van UBV en UTI.

4. Hoogte van de boete

4.1 Inleiding
Zoals in de vorige paragraaf is opgemerkt, zal de AP voor wat betreft de hoogte van de boete de voor de overtreder gunstigste bepaling toepassen door aan te sluiten bij het boeteregime van de Wbp. In het hiernavolgende zal de AP eerst kort de boetesystematiek uiteenzetten, gevolgd door de bepaling van de boetehoogte in het onderhavige geval.

4.2 De systematiek
Volgens artikel 66, tweede lid, van de Wbp gold in geval van overtreding van artikel 34a, eerste en tweede lid, van de Wbp een geldboete van ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht. Volgens artikel 23, vierde lid, van het Wetboek van Strafrecht bedraagt het maximum van de geldboete van de zesde categorie per 1 januari 2016: € 820.000.

[125] Bijlage 1 bij de schriftelijke zienswijze van Uber van 3 juli 2018.
[126] Idem.

De AP heeft 'Boetebeleidsregels Autoriteit Persoonsgegevens 2016' (Boetebeleidsregels) vastgesteld inzake de invulling van de bevoegdheid tot het opleggen van een bestuurlijke boete, waaronder het bepalen van de hoogte daarvan.[127] In de Boetebeleidsregels is gekozen voor een categorie-indeling en bandbreedte systematiek.

De beboetbare bepalingen op de naleving waarvan de AP toezicht houdt, zijn per wettelijk boetemaximum van € 820.000, € 450.000 of € 20.500 ingedeeld in een aantal boetecategorieën, en daaraan verbonden in hoogte oplopende boetebandbreedtes.

De boetecategorieën zijn gerangschikt naar zwaarte van de overtreding van de genoemde artikelen, waarbij categorie I de minst zware overtredingen bevat en categorie II of III de zwaarste overtredingen. Overtreding van artikel 34a, eerste lid, Wbp en overtreding van artikel 34a, tweede lid , Wbp zijn beide ingedeeld in categorie II.

Binnen de bandbreedte stelt de AP een basisboete vast. Als uitgangspunt geldt dat de AP de basisboete vaststelt op 33% van de bandbreedte van de aan de overtreding gekoppelde boetecategorie.[128]

De hoogte van de boete stemt de AP vervolgens af op de factoren die zijn genoemd in artikel 6 van de Boetebeleidsregels, door het basisbedrag te verlagen of verhogen. In beginsel wordt daarbij binnen de bandbreedte van de aan die overtreding gekoppelde boetecategorie gebleven. 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, zoals de (financiële) omstandigheden waarin de overtreder verkeert. De AP kan daarbij, zo nodig en afhankelijk van de mate waarin de factoren die zijn genoemd in artikel 6 van de Boetebeleidsregels daartoe aanleiding geven, de boetebandbreedte van de naast hogere respectievelijk de naast lagere categorie toepassen.

4.3 De categorie-indeling en de basisboete

Uit bijlage 1 behorende bij artikel 2 van de Boetebeleidsregels volgt dat de overtreding van artikel 34a, eerste lid, van de Wbp en de overtreding van artikel 34a, tweede lid, Wbp zijn ingedeeld in categorie II. De AP stelt de basisboete voor overtredingen waarvoor een wettelijk boetemaximum van € 820.000 geldt en die is ingedeeld in categorie II vast binnen een boetebandbreedte tussen € 120.000 en € 500.000. In dit geval wordt de basisboete per overtreding vastgesteld op € 246.500.

Ernst van de overtreding

Volgens artikel 6, eerste lid, van de Beleidsregels houdt de AP rekening met de ernst van de overtreding. Bij de beoordeling van de ernst van de overtreding betrekt de AP onder meer de aard en omvang van de

[127] Beleidsregels van de Autoriteit Persoonsgegevens van 15 december 2015, zoals laatstelijk gewijzigd op 6 juli 2016, met betrekking tot het opleggen van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2016), *Stcrt.* 2016, 2043.
[128] Boetebeleidsregels, p. 10-11.

overtreding, de duur van de overtreding en de impact van de overtreding op de betrokkenen en/of de maatschappij.[129]

Ingevolge artikel 34a, eerste lid, Wbp, zoals die bepaling gold ten tijde van de overtreding, dient de verantwoordelijke de AP onverwijld in kennis te stellen van een inbreuk op de beveiliging, bedoeld in artikel 13 Wbp, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.
Ingevolge artikel 34a, tweede lid, Wbp, zoals die bepaling gold ten tijde van de overtreding, dient de verantwoordelijke de betrokkenen onverwijld in kennis te stellen van een inbreuk op de beveiliging, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.
Het doel van de meldplicht is het voorkomen van datalekken en, als deze zich toch voordoen, de gevolgen ervan voor de betrokkenen zoveel mogelijk te beperken. Met de meldplicht wordt bijgedragen aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.[130]
Transparantie over de aard van het datalek, de vermoedelijke omvang ervan en aard van de mogelijke schade, de inspanningen die gepleegd worden om de schade te herstellen en raadgevingen aan publiek en klanten om zichzelf zo goed mogelijk in staat te stellen de consequenties voor de eigen belangen te overzien zijn noodzakelijke maatregelen voor behoud en herstel van dat vertrouwen. Dat vertrouwen wordt ondersteund doordat de AP in staat moet worden gesteld zich een eigen beeld te vormen van de feiten, een oordeel kunnen geven over de genomen maatregelen, onder omstandigheden vertrouwelijk met de verantwoordelijke kunnen overleggen en zo nodig kunnen interveniëren.[131]
Volledigheidshalve wordt in dit verband opgemerkt dat, gelet op de overwegingen 85 tot en met de 88 uit de considerans van de AVG, met de meldplicht op basis van artikel 33 en 34 AVG een vergelijkbaar doel wordt nagestreefd.

UBV en UTI hebben in de periode van 15 november 2016 tot in ieder geval 21 november 2017 nagelaten de betrokkenen onverwijld in kennis te stellen van het datalek. Pas op 21 november 2017 heeft UTI de betrokkenen middels een nieuwsbericht geïnformeerd. Daardoor de betrokkenen niet (tijdig) in staat gesteld de consequenties voor de eigen belangen te overzien door bijvoorbeeld alert te zijn op het risico op (spear)fishing. Daarnaast hebben de betrokkenen geen, althans hebben zij niet tijdig, voorzorgsmaatregelen kunnen treffen om potentieel ongunstige gevolgen van het datalek te mitigeren. Dit acht de AP ernstig.

De AP heeft bij de beoordeling van de ernst van het niet onverwijld melden van het datalek tevens de omvang van het datalek in aanmerking genomen. Het datalek treft een groot aantal personen, 57 miljoen betrokkenen wereldwijd en 174.000 Nederlandse betrokkenen. Alleen de omvang van het datalek had UTI en UBV aanleiding moeten geven om de AP en betrokkenen in kennis te stellen. Het datalek betreft voorts een grote hoeveelheid persoonsgegevens waaronder namen, e-mailadressen en mobiele telefoonnummers. Deze omstandigheden maken dat het datalek ernstige nadelige gevolgen voor de

[129] Dit sluit overigens aan bij het criterium uit artikel 83, tweede lid, sub a, AVG.
[130] *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 1.
[131] *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 4.

bescherming van persoonsgegevens had, althans had kunnen hebben. Naar het oordeel van de AP is door de overtreding het vertrouwen in de omgang met persoonsgegevens in ernstige mate geschaad.

Daar komt bij dat UBV en UTI in elk geval 72 uur na ontdekking van het datalek op 14 november 2016, tot 21 november 2017, hebben nagelaten de AP in kennis te stellen van de inbreuk op de beveiliging. Aldus is de AP gedurende een langere periode niet op de hoogte geweest van het (omvangrijke) datalek. De AP heeft zich derhalve niet (tijdig) een eigen beeld kunnen vormen van de feiten en de eventuele door Uber genomen maatregelen, zowel richting betrokkenen als wat betreft de noodzakelijke afhandeling van het (acute)beveiligingslek. Door dit nalaten van UTI en UBV is de AP ernstig belemmerd in haar toezichtsuitoefening, waarmee indirect ook de belangen van betrokkenen gemoeid zijn.

De AP ziet per saldo aanleiding om het basisbedrag van de boete, op grond van de mate van ernst van de overtreding, per overtreding te verhogen met een derde tot €327.845.

Mate van verwijtbaarheid van de overtreder
Volgens artikel 6, tweede lid, van de Beleidsregels houdt de AP rekening met de mate waarin de overtreding aan de overtreder kan worden verweten.[132] Indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid als bedoeld in artikel 66, vierde lid, van de Wbp, wordt aangenomen dat sprake is van een aanzienlijke mate van verwijtbaarheid van de overtreder.

Zoals de AP hierboven reeds uiteen heeft gezet, is de AP van oordeel dat sprake is van ernstig verwijtbare nalatigheid aan de zijde van UTI en UBV. Kort samengevat komt het erop neer dat men binnen de top van het Uber-concern op de hoogte was van het datalek, men doordrongen was van de ernst daarvan en er geen misverstand over kon bestaan dat de AP en betrokkenen onverwijld van het datalek in kennis hadden moeten worden gesteld. Desondanks was het Uber-concern er alles aan gelegen om het datalek geheim te houden, waartoe Uber bereid is geweest om een substantieel hoger geldbedrag dan normaal gebruikelijk aan melders te betalen en met de melders aanvullende geheimhoudingsverplichtingen overeen te komen. Pas ruim een jaar na ontdekking van het datalek bij UTI is het datalek op 21 november 2017 door UBV gemeld aan de AP en is op de website van Uber een nieuwsbericht gepubliceerd door de huidige CEO van UTI waarin het publiek wordt ingelicht over het datalek. Gezien het voorgaande is de AP van oordeel dat sprake is van een aanzienlijke mate van verwijtbaarheid.

De AP ziet daarom aanleiding om het basisbedrag van de boete, op grond van de mate van verwijtbaarheid per overtreding te verhogen met een derde.

Met de voorgaande stappen komt het boetebedrag op € 409.190 per overtreding, zodat het totale boetebedrag op € 818.380 uit zou komen.

Evenredigheid
Tot slot beoordeelt de AP op grond van het in artikel 5:46 van de Algemene wet bestuursrecht gecodificeerde evenredigheidsbeginsel of de toepassing van haar beleid voor het bepalen van de hoogte

[132] Dit sluit overigens aan bij het criterium uit artikel 83, tweede lid, sub b, AVG.

van de boete gezien de omstandigheden van het concrete geval, niet tot een onevenredige uitkomst leidt. Toepassing van het evenredigheidsbeginsel kan volgens de Boetebeleidsregels van de AP onder andere spelen bij de cumulatie van sancties. Indien de AP voor te onderscheiden, maar wel samenhangende overtredingen twee of meer boetes wil opleggen, moet het totaal van de boetes nog wel aansluiten bij de ernst van de overtredingen.[133]

In dit geval gaat de AP over tot boeteoplegging voor overtreding van zowel artikel 34a, eerste lid en tweede lid, van de Wbp. Naar het oordeel van de AP zijn dit te onderscheiden overtredingen. Immers, artikel 34a, eerste lid, van de Wbp vereist dat de AP onverwijld in kennis wordt gesteld van een datalek terwijl artikel 34a, tweede lid, van de Wbp vereist dat de betrokkenen onverwijld in kennis worden gesteld van een datalek. Tegelijkertijd onderkent de AP dat de strekking van de desbetreffende bepalingen in de kern gelijkwaardig is, namelijk transparantie met het oogmerk om het vertrouwen in de omgang met persoonsgegevens te behouden en/of te herstellen. Voorts is de AP van oordeel dat de gedragingen die aan de overtredingen ten grondslag liggen in essentie op hetzelfde feitencomplex zijn gebaseerd. Dit geeft aanleiding om het hierboven genoemde boetebedrag op grond van de evenredigheid te matigen.

Bij de beoordeling van de evenredigheid betrekt de AP in dit geval ook het feit dat, ondanks het tijdsverloop en het uitblijven van een bindende aanwijzing, het datalek uiteindelijk wel openbaar is geworden en de afdoening ervan de nodige media-aandacht heeft gehad zodat betrokkenen er kennis van hebben kunnen nemen.

Aldus stelt de AP het totale boetebedrag vast op € 600.000. Dit bedrag kan Uber gezien haar financiële positie dragen.

5. Dictum

De AP legt aan het UBV en UTI gezamenlijk, wegens overtreding van artikel 34a, eerste en tweede lid, Wbp, een bestuurlijke boete op ten bedrage van **€ 600.000**, voor de betaling waarvan zij hoofdelijk aansprakelijk zijn.

UBV en/of UTI dien(t)(en) het bedrag binnen zes weken over te maken op bankrekening [VERTROUWELIJK] ten name van Autoriteit Persoonsgegevens, onder vermelding van zaaknummer [VERTROUWELIJK]. UBV en UTI ontvangen geen afzonderlijke factuur voor dit bedrag.

De boete moet worden betaald binnen zes weken na de datum van dit besluit.[134] Als UBV en/of UTI bezwaar maak(t)(en) tegen dit besluit wordt de verplichting om de boete te betalen geschorst totdat op het bezwaar is beslist. Die verplichting wordt ook geschorst als UBV en/of UTI na de bezwaarprocedure in beroep gaat/gaan, totdat op het beroep is beslist.[135]

[133] Boetebeleidsregels, p. 11.
[134] Zie artikel 4:87, eerste lid, en de artikelen 3:40 en 3:41 van de Awb.
[135] Zie artikel 71 Wbp.

Datum
6 november 2018

Ons kenmerk
[VERTROUWELIJK]

De Autoriteit Persoonsgegevens,
Namens deze,

w.g.

mr. A. Wolfsen
Voorzitter

Rechtsmiddelenclausule
Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag, onder vermelding van “Awb-bezwaar” op de envelop.