COMMAND ALKON INCORPORATED - BIJLAGE GEGEVENSBESCHERMING

Bijgewerkt op: 21 juli 2022

Deze bijlage Gegevensbescherming ("**DPA**") is onderdeel van de *Hoofdlicentie- en serviceovereenkomst* ("**Overeenkomst**") tussen: (i) de Klant (genoemd op de handtekeningregel hieronder) en zijn in de EER gevestigde gelieerde partijen **(**"**Klant**"**)**; en (ii) Command Alkon Incorporated en zijn gelieerde partijen ("**Bedrijf**").

Omwille van de toepasselijke Algemene verordening gegevensbescherming (de "AVG") vervangt deze Bijlage alle eerdere overeenkomsten tussen de partijen over het betreffende onderwerp in deze, namelijk de privacy en beveiliging van gegevens voor zover toepasselijk onder de AVG.

Gelet op de wederzijdse verplichtingen die hierin zijn beschreven, komen de partijen hierbij overeen dat de hieronder beschreven algemene voorwaarden als Bijlage aan de Overeenkomst zullen worden toegevoegd.

1. Definities

"**Persoonsgegevens van de klant**" betekent persoonsgegevens die het Bedrijf namens de Klant Verwerkt bij het leveren van de Producten en/of Services.

"**Betrokkene**" betekent het individu op wie de Persoonsgegevens van de klant betrekking hebben.

"**Gegevensbeschermingswetgeving**" betekent de Algemene Verordening Gegevensbescherming (EU) 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (en alle amendementen of vervangingen), de Zwitserse Federale gegevensbeschermingswet van 19 juni 1992 (en alle amendementen en vervangingen), of de Europese AVG zoals geamendeerd en opgenomen in de Britse wetgeving onder de Britse terugtrekkingswet (uit de EU) van 2018 en de toepasselijke secundaire wetgeving onder die wet (en alle amendementen of vervangingen), al naargelang van toepassing

"**Persoonsgegevens**" betekent alle informatie over een Betrokkene, met inbegrip van, maar niet beperkt tot een naam, een identificatienummer, locatiegegevens, een online identificatienummer, of een of twee factoren specifiek voor de fysieke, fysiologische, genetische, verstandelijke, economische, culturele of maatschappelijke identiteit van de Betrokkene

"**Privacyschild**" betekent het juridische privacyschildkader tussen de EU en de VS en het juridische privacyschildkader tussen Zwitserland en de VS. Hoewel beide kaders momenteel onuitvoerbaar zijn, blijft het Bedrijf zich houden aan de voorschriften, en zal dit begrip van toepassing zijn op alle hernieuwde en goedgekeurde versies van de privacyschildovereenkomst tussen de Verenigde Staten en de Europese Economische Ruimte ("EER").

"**Verwerking**" of "**Verwerken**" betekent alle bewerkingen of serie bewerkingen die, al dan niet met behulp van automatische middelen, worden uitgevoerd op Persoonsgegevens van de klant, zoals het verzamelen, opnemen, ordenen, structureren, bewaren, wijzigen, ophalen, raadplegen, gebruiken, openbaar maken, verwijderen, beperken, openen, verspreiden, combineren, aanpassen, kopiëren, doorgeven, wissen en/of vernietigen van Persoonsgegevens van de klant.

"**Beveiligingsschending**" betekent een schending van de beveiliging met als gevolg het onopzettelijk of onrechtmatig vernietigen, verliezen, wijzigen, onbevoegd openbaar maken of openen van doorgegeven, opgeslagen of anderszins verwerkte Persoonsgegevens van de klant.

"Derde" betekent een andere partij dan de Klant of het Bedrijf.

De begrippen "**verwerkingsverantwoordelijke**", "**verwerker**" en "**toezichthoudende autoriteit**" zoals gebruikt in deze DPA hebben de betekenis die er in de AVG aan gegeven wordt.

Alle andere niet-gedefinieerde maar met hoofdletters beginnende begrippen hebben de betekenis die in de Overeenkomst is aangegeven.

2. Verwerken van Persoonsgegevens van de klant

2.1 Verwerkingsdoel. Het doel van de Verwerking van gegevens onder deze DPA is het leveren van de Producten en/of Services op grond van de Overeenkomst. Bijlage 1 beschrijft het onderwerp en de bijzonderheden van het Verwerken van Persoonsgegevens van de klant.

2.2 Verantwoordelijkheden van de Verwerker en de Verwerkingsverantwoordelijke. De partijen erkennen en stemmen ermee in dat: (a) het Bedrijf een Verwerker van Persoonsgegevens is onder de Gegevensbeschermingswetgeving; (b) de Klant een verwerkingsverantwoordelijke van Persoonsgegevens van de klant is onder de Gegevensbeschermingswetgeving; en (c) elke partij aan de betreffende verplichtingen zal voldoen onder de Gegevensbeschermingswetgeving inzake de Verwerking van Persoonsgegevens van de klant.

2.3 Instructies van de Klant. De Klant geeft het Bedrijf instructie om Persoonsgegevens van de klant te Verwerken: (a) conform de Overeenkomst en alle toepasselijke Bijlagen; (b) op andere wijze die noodzakelijk is om producten en/of services aan de Klant te leveren; (c) indien noodzakelijk om te voldoen aan toepasselijke wet- en regelgeving of voorschriften; en (d) om te voldoen aan andere redelijke schriftelijke instructies van de Klant waar die instructies in overeenstemming zijn met de bepalingen van de Overeenkomst. De Klant zal waarborgen dat zijn instructies voor het Verwerken van Persoonsgegevens van de klant zullen voldoen aan de Gegevensbeschermingswetgeving. Tussen beide partijen is de Klant volledig verantwoordelijk voor de nauwkeurigheid, kwaliteit en rechtmatigheid van de Persoonsgegevens van de klant en de middelen die de Klant heeft gebruikt om de Persoonsgegevens van de klant te verkrijgen.

2.4 Naleving van de instructies van de Klant door het Bedrijf Het Bedrijf zal de Persoonsgegevens van de klant uitsluitend volgens de instructies van de Klant Verwerken en zal de Persoonsgegevens van de klant als vertrouwelijke informatie behandelen. Als het Bedrijf meent te weten of te weten komt dat een instructie van de Klant in strijd is met de Gegevensbeschermingswetgeving, zal het Bedrijf de Klant hierover binnen redelijke termijn inlichten. Het Bedrijf kan Persoonsgegevens van de klant anders Verwerken dan op schriftelijke instructie van de Klant als de toepasselijke wet- en regelgeving waaronder het Bedrijf valt, dit verplicht. In dat geval zal het Bedrijf de Klant inlichten over zulke verplichtingen alvorens het Bedrijf de Persoonsgegevens van de klant Verwerkt, tenzij dit door de toepasselijke wet is verboden.

3. Subverwerkers

3.1 Benoeming van subverwerkers. De Klant verleent hierbij algemene schriftelijke toestemming aan het Bedrijf om externe subverwerkers in te huren die beperkte of aanvullende services bieden in verband met het leveren van producten en/of services. De website van het Bedrijf vermeldt subverwerkers die momenteel door het Bedrijf zijn ingehuurd om specifieke verwerkingsactiviteiten uit te voeren op Persoonsgegevens van de klant en het Bedrijf zal de subverwerkerslijst bijwerken alvorens nieuwe subverwerkers in te huren voor uitvoering van specifieke verwerking. Telkens wanneer de subverwerkerslijst van het Bedrijf is gewijzigd, kan de Klant zich opgeven voor elektronische updates. De Klant kan binnen dertig (30) dagen na een update bezwaar indienen bij het Bedrijf tegen een subverwerker, waarna de partijen te goeder trouw samen aan een oplossing van het probleem werken. De Klant gaat hierbij akkoord met de subverwerkersactiviteiten door de momenteel vermelde subverwerkers op de websitelijst van het Bedrijf.

3.2 Beveiliging subverwerkers In het geval dat het Bedrijf zijn verplichtingen uitbesteedt, zal het dit uitsluitend doen door een schriftelijke overeenkomst aan te gaan waarin de subverwerker contractuele verplichtingen wordt opgelegd die ten minste gelijk zijn aan de verplichtingen in deze Bijlage.

3.3 Aansprakelijkheid. In het geval dat de subverwerker niet voldoet aan zijn verplichtingen onder die schriftelijke overeenkomst, zal het Bedrijf ten opzichte van de Klant volledig aansprakelijk blijven ten aanzien van de uitvoering van de verplichtingen onder die overeenkomst.

4. Beveiligings- en privacyeffectbeoordelingen

4.1 Beveiliging bij het Bedrijf. Het Bedrijf zal toereikende technische en organisatorische maatregelen treffen om de Persoonsgegevens van de klant te beschermen (“Informatiebeveiligingsprogramma”) rekening houdend met de nieuwste mogelijkheden, de implementatiekosten en de aard, reikwijdte, context en het doel van Verwerking, alsmede de variërende kans op en ernst van het risico die de rechten en vrijheden van natuurlijke personen lopen. De huidige technische en organisatorische maatregelen van het Bedrijf zijn vermeld in Bijlage II van de Modelcontractbepalingen (bijgevoegd). Het Bedrijf is zelfsturend met gebruikmaking van de volgende beveiligingsnormen: NIST 800-171; AWS CIS.

4.2 Beveiliging bij de Klant. De Klant erkent naar wens bepaalde functies en functionaliteiten in de producten en/of services te kunnen gebruiken die van invloed zijn op de beveiliging van Persoonsgegevens van de klant als de Klant de producten en/of services gebruikt. De Klant is verantwoordelijk voor het bestuderen van de informatie die het Bedrijf beschikbaar stelt over zijn gegevensbeveiliging en het onafhankelijk bepalen of de producten en/of services voldoen aan de eisen en wettelijke verplichtingen van de Klant, met inbegrip van zijn verplichtingen onder de toepasselijke Gegevensbeschermingswetgeving. Verder is de Klant verantwoordelijk voor het correct configureren van de producten en/of services en het gebruik van functies en functionaliteiten die het Bedrijf beschikbaar stelt om, gelet op de aard van de Verwerking van Persoonsgegevens van de klant, toereikende beveiliging te handhaven die past bij het gebruik van de producten en/of services door de Klant. De Klant is verantwoordelijk voor zijn gebruik van de producten en/of services en het opslaan van alle kopieën van Persoonsgegevens van de klant buiten het Bedrijf of de systemen van de subverwerkers van het Bedrijf, met inbegrip van, maar niet beperkt tot beveiliging van de verificatiereferenties van accounts, systemen en apparaten, en het bewaren van kopieën van Persoonsgegevens van de klant, naar gelang van toepassing.

4.3 Personeel van het Bedrijf. Het Bedrijf zal waarborgen dat het betrokken personeel bij het Verwerken van Persoonsgegevens van de klant het vertrouwelijke karakter van de Persoonsgegevens van de klant kent en weet dat ze een geheimhoudingsplicht hebben, een geheimhoudingsplicht die van kracht blijft na beëindiging van de betrekkingen met het Bedrijf.

4.4 Testen van beveiliging. Het Bedrijf zal de effectiviteit van het Informatiebeveiligingsprogramma testen, beoordelen en evalueren om het veilig Verwerken van Persoonsgegevens van de klant te waarborgen. Het Bedrijf zal zich aan zijn Informatiebeveiligingsprogramma houden en verklaart en garandeert dat zijn Informatiebeveiligingsprogramma voldoet en zal blijven voldoen aan de toepasselijk wetgeving.

4.5 Effectbeoordelingen. Het Bedrijf zal redelijke stappen ondernemen om medewerking te verlenen aan de Klant bij het uitvoeren van effectbeoordelingen en de eraan gekoppelde advisering ten behoeve van een toezichthoudende autoriteit als van de Klant wordt geëist om een effectbeoordeling onder de Gegevensbeschermingswetgeving uit te voeren.

5. Rechten van een Betrokkene

5.1 Hulp bij verplichtingen van de Klant. Voor zover de Klant bij zijn gebruik of ontvangst van de producten en/of services niet over de mogelijkheden beschikt om Persoonsgegevens van de klant te corrigeren, aanvullen, beperken, blokkeren of verwijderen volgens de vereisten van de Gegevensbeschermingswetgeving, zal het Bedrijf prompt redelijke verzoeken van de Klant inwilligen om zulke acties te faciliteren in de mate waarin het Bedrijf dit wettelijk is toegestaan en kan doen. Als het wettelijk is toegestaan, komen de kosten voor de hulp die het Bedrijf verleent voor rekening van de Klant.

5.2 Meldingsplicht. Het Bedrijf zal, voor zover wettelijk toegestaan, de Klant prompt inlichten als een Betrokkene een verzoek bij het Bedrijf indient voor inzage in, correctie van, aanvulling op, verwijdering van of bezwaar tegen het Verwerken van Persoonsgegevens van de klant over dat individu. Het Bedrijf zal niet reageren op zulke verzoeken van een Betrokkene over Persoonsgegevens van de klant zonder eerst schriftelijke toestemming te vragen van de Klant, behalve om na te gaan of het verzoek de Klant betreft. Bovendien zal het Bedrijf, voor zover wettelijk toegestaan, de Klant prompt inlichten als het een verzoek krijgt om openbaarmaking van correspondentie, kennisgeving of andere communicatie over Persoonsgegevens van de klant van wetshandhavingsautoriteiten, een bevoegde autoriteit of de betreffende gegevensbeschermingsautoriteit. Voor zover wettelijk toegestaan en voor zover de Klant geen toegang heeft tot zulke Persoonsgegevens van de klant via het gebruik of ontvangst van de producten en/of services, zal het Bedrijf in redelijke mate medewerking en hulp verlenen aan de Klant bij het afhandelen van zulke verzoeken. Als het wettelijk is toegestaan, komen de kosten voor de hulp die het Bedrijf verleent voor rekening van de Klant.

6. Inbreuk op persoonsgegevens

6.1 Meldingsplicht. In het geval dat het Bedrijf kennis krijgt van een geverifieerde Beveiligingsschending, zal het Bedrijf de Klant zonder onnodig uitstel inlichten over de Beveiligingsschending en in geen geval later dan tweeënzeventig (72) uur na ontdekking. De verplichtingen in deze paragraaf 6 zijn niet van toepassing op incidenten die worden veroorzaakt door de Klant of het personeel of de eindgebruikers van de Klant of door niet geslaagde pogingen of activiteiten die de beveiliging van Persoonsgegevens van de klant niet compromitteren, met inbegrip van niet geslaagde pogingen tot aanmelding, pingen, poortscannen, denial-of-service-aanvallen en andere netwerkaanvallen op firewalls of netwerksystemen.

6.2 Wijze van kennisgeving. Kennisgeving van eventuele Beveiligingsschendingen zullen via e-mail of telefonisch worden gedaan aan het AVG-meldpunt bij de Klant. Het is de volledige verantwoordelijkheid van de Klant om ervoor te zorgen dat de contactgegevens in de ondersteuningssystemen van het Bedrijf altijd juist zijn.

6.3 Inhoud van de kennisgeving. In het geval een kennisgeving nodig is, zal de kennisgeving minimaal:

6.3.1 de aard van de Beveiligingsschending, de categorieën en het aantal getroffen Betrokkenen, en de categorieën en het aantal getroffen personeelsrecords beschrijven;

6.3.2 de naam en contactgegevens van de contactpersoon van het Bedrijf noemen die meer informatie kan verstrekken;

6.3.3 de mogelijke gevolgen beschrijven van de Beveiligingsschending; en

6.3.4 de genomen of voorgestelde maatregelen beschrijven om de Beveiligingsschending te verhelpen.

7. Verwijderen of retourneren van Persoonsgegevens van de klant

7.1 Verwijderen of retourneren. Onverminderd het bepaalde in artikel 7.3 komt het Bedrijf overeen om prompt en in ieder geval binnen dertig (30) dagen na stopzetting van een service in het Verwerken van Persoonsgegevens van de klant (de "**Stopzettingsdatum**") veilig Persoonsgegevens van de klant te verwijderen of, als de Klant dit tijdig verzoekt, een volledige kopie van alle Persoonsgegevens van de klant aan de Klanten te retourneren in een beveiligde bestandsoverdracht in een redelijke indeling die de Klant aanvraagt.

7.2 Definitie van Verwijderen. Voor alle duidelijkheid, "**Verwijderen**" betekent het zo uitwissen of vernietigen van Persoonsgegevens dat ze niet meer te herstellen of reconstrueren zijn.

7.3 Records. Het Bedrijf kan Persoonsgegevens van de klant bewaren voor zover de toepasselijke wetgeving dit verplicht of conform de vastgestelde bewaartermijnen voor documenten van het Bedrijf, op voorwaarde dat het Bedrijf de vertrouwelijkheid van al deze Persoonsgegevens van de klant waarborgt.

8. Auditrechten

8.1 Auditrechten De Klant mag niet meer dan eenmaal per jaar en uitsluitend om te voldoen aan de auditverplichtingen op grond van artikel 28, paragraaf 3(h) van de AVG het Bedrijf laten inspecteren door een onderling overeengekomen derde. Om een audit aan te vragen, moet de Klant ten minste vier (4) weken vóór de voorgestelde auditdatum een gedetailleerd auditplan indienen waarin de voorgestelde reikwijdte, duur en startdatum van de audit zijn vermeld. Auditverzoeken moeten worden verzonden naar privacy@commandalkon.com. De controleur moet een voor het Bedrijf aanvaardbare schriftelijke geheimhoudingsverklaring overleggen alvorens de audit uit te voeren. De audit moet worden uitgevoerd tijdens normale kantooruren, voldoen aan het beleid van het Bedrijf en mag de dagelijkse gang van zaken binnen het Bedrijf niet hinderen. Alle audits zijn volledig op kosten en onkosten van de Klant. Het Bedrijf zal medewerking verlenen aan een auditverzoek van de Klant of een bevoegde autoriteit of toezichthoudende autoriteit waarin wordt gecontroleerd of het Bedrijf voldoet aan zijn verplichtingen onder deze DPA door het beschikbaar stellen van auditrapporten van derden, als deze bestaan, beschrijvingen van beveiligingsmaatregelen en andere informatie die de Klant redelijkerwijs verzoekt over praktijken en beleid inzake beveiliging, onder voorbehoud dat het Bedrijf niet gebonden is aan een geheimhoudingsverplichting.

8.2 Hulp bij naleving. Rekening houdend met de aard van de Verwerking en de informatie die het Bedrijf ter beschikking staat, zal het Bedrijf in redelijke mate medewerking en hulp verlenen aan de Klant bij de naleving door de Klant van zijn verplichtingen onder Artikelen 32-36 van de AVG.

9. Gegevensdoorgifte

9.1 Algemene toestemming. De Klant geeft het Bedrijf toestemming om, onverminderd het bepaalde in artikel 9.2, Persoonsgegevens van de klant te Verwerken in de Verenigde Staten van Amerika en alle andere landen waarin het Bedrijf of zijn

subverwerkers over faciliteiten beschikken of anderszins Persoonsgegevens Verwerken. Op al zulke doorgiften zullen de Modelcontractbepalingen tussen filialen of de privacyschildcertificatie (mocht deze weer worden ingevoerd) van het Bedrijf van toepassing zijn. Het Bedrijf zal geen Persoonsgegevens van de klant doorgeven of laten doorgeven van de ene naar een andere jurisdictie, mits dit in overeenstemming met de toepasselijke wetgeving is en niet tot gevolg heeft dat de Klant gegevensbeschermingswetten schendt.

9.2 Modelcontactbepalingen. Voor zover, en uitsluitend voor zover het Bedrijf Persoonsgegevens van de klant uit de Europese Economische Ruimte, Zwitserland of het VK Verwerkt en Modelcontractbepalingen vereist zijn, zullen de toepasselijke Modelcontractbepalingen (EER of VK) van toepassing zijn die bij deze zijn opgenomen. Ten behoeve van de Modelcontractbepalingen is de Klant "gegevensexporteur" en het Bedrijf de "gegevensimporteur". Het Bedrijf heeft de 2021 Modelcontractbepalingen geïmplementeerd tussen gelieerde partijen van het Bedrijf en zelfcertificatie gecontinueerd voor het Privacyschild (mocht deze weer worden ingesteld) voor gegevensdoorgiften naar de Verenigde Staten van Amerika.

9.3 Britse Modelcontractbepalingen. De partijen komen overeen dat de Britse Modelcontractbepalingen van toepassing zullen zijn op persoonsgegevens die via de producten en/of services worden doorgegeven vanaf het Verenigd Koninkrijk, direct dan wel door verdere doorgifte, naar landen of ontvangers buiten het Verenigd Koninkrijk die niet door de bevoegde Britse autoriteit of overheidsinstantie worden geacht een passend beschermingsniveau voor persoonsgegevens te bieden. Voor gegevensdoorgifte vanaf het Verenigd Koninkrijk waarop de Britse Modelcontractbepalingen van toepassing zijn, zullen de Britse Modelcontractbepalingen een integraal onderdeel vormen en zijn hierbij opgenomen in deze Bijlage.

9.4 Aanvullende maatregelen. Aanvullend op de Modelcontractbepalingen geldt dat mocht het Bedrijf vernemen dat een overheidsinstantie (waaronder wetshandhavingsautoriteiten) toegang tot of een kopie wenst te krijgen van alle of een deel van de Persoonsgegevens van de klant die het Bedrijf heeft Verwerkt, op vrijwillige dan wel verplichte basis, voor doeleinden die de nationale veiligheid betreffen, zal het Bedrijf, tenzij dit wettelijk niet is toegestaan of de wet verplicht anders te handelen: 1) onmiddellijk de Klant inlichten aan wie de persoonsgegevens toebehoren; 2) de betreffende overheidsinstantie informeren dat het geen toestemming heeft om de Persoonsgegevens van de klant openbaar te maken en, tenzij dit wettelijk verboden is, onmiddellijk de Klant moet inlichten aan wie de Persoonsgegevens toebehoren; 3) de overheidsinstantie inlichten dat alle verzoeken of eisen rechtstreeks aan de Klant gericht moeten worden aan wie de Persoonsgegevens toebehoren; en 4) pas toegang tot de Persoonsgegevens verstrekken, nadat het schriftelijke goedkeuring heeft ontvangen van de Klant aan wie de Persoonsgegevens toebehoren of hiertoe wettelijk verplicht is gesteld. Wanneer sprake is van een wettelijke verplichting, zal het Bedrijf binnen de wettelijke mogelijkheden redelijke inspanningen leveren om het verbod of de verplichting aan te vechten. In geval het Bedrijf wettelijke verplicht is gesteld de Persoonsgegevens van de klant op te leveren, zal het Bedrijf uitsluitend Persoonsgegevens van de klant bekendmaken voor zover wettelijk verplicht volgens de toepasselijke wettelijke procedure.

9.5 Voorrang bij doorgifte In geval de services onder meerdere doorgiftemechanismen vallen, zal één doorgiftemechanisme van toepassing zijn op de doorgifte van Persoonsgegevens van de klant en wel in de volgende rangorde: (i) de Modelcontractbepalingen van de EU (in geval verplicht gesteld door de toepasselijke Gegevensbeschermingswetgeving); (ii) de zelfcertificatie voor het Privacyschild (mocht deze weer worden ingevoerd).

10. Looptijd en beëindiging

Looptijd van de DPA Deze DPA zal ingaan op de datum van volledige tenuitvoerlegging en zal, niettegenstaande het vervallen van de looptijd van een aangeschaft abonnement, van kracht blijven tot en automatisch vervallen na verwijdering van alle Persoonsgegevens van de klant conform de beschrijving in deze DPA.

11. Niet-naleving; rechtsmiddelen; partijen

11.1 Beperking van aansprakelijkheid. Het Bedrijf is aansprakelijk voor zijn verplichtingen in deze DPA met inachtneming van de bepaling over beperking van aansprakelijkheid in de Overeenkomst.

11.2 Partijen bij deze DPA. Niets in deze DPA verleent rechten of voorrechten aan een andere persoon of entiteit dan de partijen bij deze DPA.

12. Algemene voorwaarden

Toepasselijk recht en rechtsbevoegdheid

12.1 Deze DPA zal één jaar na uitgiftedatum en vervolgens drie jaar daarna opnieuw worden bezien.

12.2 Tenzij anders verplicht door de Modelcontractbepalingen:

12.2.1 gaan de partijen hierbij akkoord met de genoemde jurisdictiekeuze in de Overeenkomst voor eventuele geschillen of claims die hoe dan ook voortvloeien uit deze Bijlage, met inbegrip van geschillen over het bestaan, de geldigheid of beëindiging ervan; en

12.2.2 zijn het recht van het voor dit doel genoemde land of gebied in de Overeenkomst van toepassing op deze Bijlage en alle niet-contractuele en andere verplichtingen die eruit voortvloeien.

Voorrangsrangorde

12.3 In het geval van strijdigheid of inconsistentie tussen deze Bijlage en de Modelcontractbepalingen waar de Modelcontractbepalingen verplicht zijn, zullen de Modelcontractbepalingen voorrang hebben.

12.4 Onverminderd het bepaalde in artikel 12.2 ten aanzien van de onderwerpen van deze Bijlage, zullen de bepalingen van deze Bijlage voorrang hebben in geval van inconsistentie tussen de bepalingen van deze Bijlage en andere overeenkomsten tussen de partijen, met inbegrip van

de Overeenkomst en, behoudens in gevallen waar uitdrukkelijk schriftelijk en namens de partijen anders overeengekomen is, met inbegrip van overeenkomsten die partijen zijn aangegaan of voornemens zijn aan te gaan na de datum van deze Bijlage.

Wijzigingen in Gegevensbeschermingswetgeving

12.5 De Klant mag:

12.5.1 door ten minste dertig (30) kalenderdagen vooraf het Bedrijf schriftelijk in kennis te stellen van tijd tot tijd varianten op de Modelcontractbepalingen voorstellen die noodzakelijk zijn ten gevolge van wijzigingen in of beslissingen van een bevoegde autoriteit onder die Gegevensbeschermingswetgeving; en

12.5.2 andere varianten op deze Bijlage voorstellen die de Klant redelijkerwijs noodzakelijk acht om aan de verplichtingen van de Gegevensbeschermingswetgeving te voldoen.

12.6 In het geval de Klant een in artikel 12.5 bedoelde kennisgeving verzendt, zullen de partijen prompt de voorgestelde varianten bespreken en in goed vertrouwen onderhandelen met de bedoeling om overeenstemming te bereiken en de voorgestelde of alternatieve varianten te implementeren om zodra dit redelijkerwijs mogelijk is aan de geïdentificeerde verplichtingen in de kennisgeving van de Klant te kunnen gaan voldoen.

Scheidbaarheid

12.7 Ingeval een bepaling in deze Bijlage ongeldig of niet-afdwingbaar blijkt te zijn, blijft deze Bijlage voor het overige in stand en van kracht. De ongeldige of niet-afdwingbare bepaling zal ofwel: (i) waar nodig worden herzien om geldigheid en afdwingbaarheid te waarborgen, waarbij de intenties van de partijen zo nauwsluitend mogelijk worden aangehouden, of, als dit niet mogelijk is; (ii) zo worden opgevat alsof het ongeldige of niet-afdwingbare deel er nooit onderdeel van hebben gevormd.

BIJLAGE I VAN DE MODELCONTRACTBEPALINGEN

A. LIJST VAN PARTIJEN

Gegevensexporteur(s)[1]: [*Identiteit en contactgegevens van de gegevensexporteur(s) en, indien van toepassing, van de functionaris voor gegevensbescherming en/of de vertegenwoordiger in de Europese Unie]*

Naam:

Adres:

Naam, functie en contactgegevens contactpersoon:

Activiteiten die relevant zijn voor de doorgegeven gegevens onder deze bepalingen:

Handtekening en datum:

Rol: Verwerkingsverantwoordelijke

Gegevensimporteur(s): [*Identiteit en contactgegevens van de gegevensimporteur(s), met inbegrip van alle contactpersonen die verantwoordelijk zijn voor gegevensbescherming]*

Naam: Command Alkon Incorporated

Adres: 1800 Industrial Park Drive, Suite 400, Birmingham, Alabama 35243 VS

Naam, functie en contactgegevens contactpersoon: David R. Burkholder, Associate General Counsel and Chief Privacy Officer, dburkholder@commandalkon.com, +1-205-263-5524 tst. 2837

Activiteiten die relevant zijn voor de doorgegeven gegevens onder deze bepalingen:

Chief Privacy Officer voor nalevingszaken

Handtekening en datum:

Rol: Verwerker

B. BESCHRIJVING VAN DOORGIFTE

Categorieën van Betrokkenen over wie persoonsgegevens worden doorgegeven

[1] Als dit onderdeel niet ingevuld is, zal de gegevensexporteur worden genoemd in de bijbehorende Hoofdlicentie- en servicesovereenkomst en bijbehorende documenten.

Werknemers van de Klant, klanten van de Klant, werknemers of zakenpartners van de Klant.

Categorieën van doorgegeven persoonsgegevens

Contactgegevens; gegevens over de website, het product en service-interactie; adressen; geboortedatum; geboorteplaats; e-mailadressen; namen; geslacht; titel; telefoonnummers; rijbewijsnummer; handtekening; personeelsnummer; gegevens over de geo-locatie; loonschaal; gebruikersnaam; wachtwoord; prestatiegegevens; competenties en beperkingen.

Doorgegeven gevoelige gegevens (indien van toepassing) en toegepaste beperkingen en veiligheidsmaatregelen die volledige rekening houden met de aard van de gegevens en de bijbehorende risico's, zoals bijvoorbeeld strikte beperkingen van het doel, toegangsbeperkingen (waaronder uitsluitend toegang voor personeel dat gespecialiseerde training heeft gevolgd), records bijhouden van de toegang tot de gegevens, beperking van verdere doorgifte of extra beveiligingsmaatregelen

Volgens de definitie van de AVG worden geen gevoelige gegevens doorgegeven.

De frequentie van de doorgifte (bijv. of dit eenmalig of op continue basis is).

Continue gegevensdoorgifte, omdat het product/platform gebruikt wordt door eindgebruikers.

Aard van de verwerking

Naargelang nodig voor het leveren van het product of verlenen van de service onder de Overeenkomst en volgens instructies van de exporteur.

Doel(en) van de gegevensdoorgifte en verdere verwerking

Naargelang nodig voor het leveren van het product/service of ter ondersteuning van het product of de service.

De bewaartermijn voor de persoonsgegevens, of, als dit niet mogelijkheid is, de gebruikte criteria die de bewaartermijn bepalen.

Voor de vereiste periode om het product/service te leveren en in combinatie met het beleid over of het schema van de bewaartermijnen of zoals dit door de toepasselijke wet- en regelgeving of de voorschriften is vereist.

Voor doorgifte aan (sub)verwerkers moet ook het onderwerp, de aard en de duur van de verwerking worden gespecificeerd.

Voor het leveren van de vereiste product/service-ondersteuning (bijv. cloudopslag) en voor de vereiste periode waarin het product/de service wordt geleverd.

C. DE BEVOEGDE TOEZICHTHOUDENDE AUTORITEIT

Benoem in overeenstemming met bepaling 13 de bevoegde toezichthoudende autoriteit(en)

De Autoriteit Persoonsgegevens van Nederland

BIJLAGE II VAN DE MODELCONTRACTBEPALINGEN

TECHNISCHE EN ORGANISATORISCHE MAATREGELEN, WAARONDER TECHNISCHE EN ORGANISATORISCHE MAATREGELEN OM DE BEVEILIGING VAN GEGEVENS TE WAARBORGEN

Beschrijving van de geïmplementeerde technische en organisatorische maatregelen door de importeur(s) (met inbegrip van relevante certificaties) om een passend niveau van beveiliging te verzekeren, rekening houdend met de aard, reikwijdte, context en doel van de Verwerking en de risico's die de rechten en vrijheden van natuurlijke personen lopen.

Maatregelen die persoonsgegevens pseudonimiseren en versleutelen **Versleutelen tijdens doorgifte en at-rest is geïmplementeerd**

Maatregelen die continue geheimhouding, integriteit, beschikbaarheid en de veerkracht van verwerkingssystemen en -services waarborgen **Command Alkon is zelfsturend met gebruikmaking van het NIST 800-171-beveiligingskader, de AWS CIS Benchmarks v1.2 en AWS Foundational Best Practices v1.0**

Maatregelen ten behoeve van een tijdig herstel van de beschikbaarheid en toegang tot persoonsgegevens in geval van een fysiek of technisch incident **Command Alkon voert regelmatig geplande back-ups uit en beschikt over een architectuur gericht op maximale beschikbaarheid**

Procedures ten behoeve van het regelmatig testen, beoordelen en evalueren van de effectiviteit van de technische en organisatorische maatregelen om de veiligheid van verwerking te waarborgen **Periodieke geautomatiseerde kwetsbaarheidstesten; jaarlijkse penetratietesten; jaarlijkse privacy- en beveiligingsaudits**

Maatregelen ten behoeve van identificatie en verificatie van gebruikers **Multifactorverificatie; geavanceerd wachtwoordprogramma; beperking van rechten; logboeken**

Maatregelen ten behoeve van het beveiligen van gegevens tijdens doorgifte **Versleuteling tijdens doorgifte**

Maatregelen voor het beveiligen van gegevens in opslag **At-rest versleuteling; logische toegangsbeveiligingen; redundantie via back-up en failover**

Maatregelen ten behoeve van de fysieke beveiliging van locaties waar personeelsgegevens worden verwerkt **Toegangspasjes/codes; bezoekersregistratie; videobewaking; bewakingspersoneel; training in beveiliging/privacy**

Maatregelen ten behoeve van logboekregistratie van gebeurtenissen **Logboekregistratie is geïmplementeerd en wordt bewaakt; logboeken worden via een feed naar een externe, beheerde service verzonden; gebeurteniswaarschuwingen zijn ingeschakeld**

Maatregelen die de systeemconfiguratie waarborgen, waaronder de standaardconfiguratie **Elke status en wijziging van de configuratie wordt bijgehouden; veranderingsmanagement geïmplementeerd**

Maatregelen ten behoeve van de governance en het beheer van interne IT en IT-beveiliging **Beveiligings- en privacy-beleid en -procedures; Chief Information Security Officer; gespecialiseerd SecOps-team; Chief Privacy Officer; training in beveiliging/privacy**

Maatregelen ten behoeve van certificering/borging van procedures en producten **NIST 800-171; CIS AWS Benchmark v1.2; AWS Foundational Best Practices v1.0**

Maatregelen ten behoeve van gegevensminimalisering **Gegevens worden uitsluitend op door de eindgebruiker/klant/Verwerkingsverantwoordelijke ingevoerde velden verwerkt**

Maatregelen ten behoeve van gegevenskwaliteit **Gegevens worden door de eindgebruiker/klant/Verwerkingsverantwoordelijke ingevoerd**

Maatregelen ten behoeve van beperkte tijd bewaren van gegevens **Het bewaren van gegevens gebeurt op grond van contractuele verplichtingen en het beleid over of het schema van de bewaartermijnen**

Maatregelen ten behoeve van de verantwoordingsplicht **De verantwoordingsplicht wordt vervuld door middel van bewaakte logboekregistratie; logboeken worden via een feed naar een externe, beheerde service verzonden; gebeurteniswaarschuwingen zijn ingeschakeld**

Maatregelen die gegevensportabiliteit mogelijk maken en wissen verzekeren **Gegevensportabiliteit wordt gevalsgewijs afgehandeld en contractuele verplichtingen en procedures voor 'kennisgeving-en-bevestiging' waarborgen wissen**

Beschrijf voor doorgifte aan (sub)verwerkers ook de specifieke technisch en organisatorisch te nemen maatregelen door de (sub)verwerker om hulp te mogen verlenen aan de verwerkingsverantwoordelijke en, voor doorgifte van gegevens door een verwerker naar een subverwerker naar de gegevensexporteur

Subverwerkers die persoonsgegevens verwerken, zijn gebonden aan contractuele beperkingen en bijlagen waarin, indien van toepassing, naleving van de Modelcontractbepalingen verplicht wordt gesteld voor gegevensverwerking