COMMAND ALKON INCORPORATED, ADDENDUM OVER GEGEVENSVERWERKING

Bijgewerkt: 25/07/24

Dit addendum voor gegevensverwerking („**DPA** „) maakt deel uit van de *hoofdlicentie- en dienstenovereenkomst („***Overeenkomst**") tussen: (i) de klant (geïdentificeerd in de hoofdlicentie- en dienstenovereenkomst) en zijn aan de EER gelieerde ondernemingen **("Klant"); en (ii)** Command Alkon Incorporated en zijn dochterondernemingen (" **Bedrijf** „), alleen indien vereist op grond van de Algemene Verordening Gegevensbescherming („**GDPR**") of andere toepasselijke privacy wetgeving.

Dit addendum vervangt elke eerdere overeenkomst tussen de partijen over het onderwerp in dit document, dat wil zeggen gegevensprivacy en -beveiliging, zoals van toepassing op de privacywetgeving.

Met het oog op de wederzijdse verplichtingen die hierin zijn uiteengezet, komen de partijen hierbij overeen dat de onderstaande voorwaarden als bijlage bij de overeenkomst worden toegevoegd.

1. Definities

„**Persoonlijke gegevens van klanten**" betekent persoonsgegevens die door het bedrijf namens de klant worden verwerkt om de producten en/of diensten te leveren.

„**CCPA**" betekent de California Consumer Privacy Act, zoals gewijzigd door de California Privacy Rights Act of verdere Californische wet/regelgeving.

„**Betrokkene**" betekent de persoon op wie de persoonsgegevens van de klant betrekking hebben.

„Data Privacy Framework" betekent het rechtskader tussen de EU en de VS voor grensoverschrijdende overdracht van persoonsgegevens tussen de Europese Unie en de Verenigde Staten, met inbegrip van de Britse uitbreiding naar de EU-VS. DPF en de Swiss-U.S. PDF.

„**Gegevensbeschermingswetten**" betekent alle toepasselijke wet- en regelgeving met betrekking tot de verwerking van persoonsgegevens en privacy die kunnen bestaan in de relevante rechtsgebieden, waaronder, indien van toepassing, 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 dergelijke gegevens, en tot intrekking van Richtlijn 95/46/EG („GDPR") (en elke wijziging of vervanging ervan), de Zwitserse federale wet inzake Gegevensbescherming („FADP") (en elke wijziging of vervanging ervan)), de GDPR van de EU zoals gewijzigd en opgenomen in de Britse wetgeving op grond van de Britse wet inzake terugtrekking van 2018 en de toepasselijke secundaire wetgeving op grond van die wet („Britse GDPR") (en elke wijziging of vervanging ervan), de Canadese wet op de bescherming van persoonsgegevens en elektronische documenten („PIPEDA") (en elke wijziging of vervanging ervan), de Braziliaanse algemene wet inzake gegevensbescherming (de „LGPD") (en elke wijziging of

vervanging ervan), de Privacywet 1988 (Cth) van Australië, zoals gewijzigd („Australische privacywet") (en elke wijziging of vervanging ervan), U.S. de privacywetgeving van de staat (waaronder de CCPA en de CPRA van Californië) zoals uitgevaardigd of gewijzigd, of elke andere toepasselijke privacywetgeving die een gegevensbeschermingsautoriteit vereist. Wanneer de GDPR specifiek wordt genoemd, zijn dezelfde vereisten van toepassing op alle andere gelijkwaardige vereisten van de toepasselijke wetgeving inzake gegevensbescherming.

„**Persoonsgegevens**" betekent alle informatie die betrekking heeft op een Betrokkene, met inbegrip van maar niet beperkt tot een naam, een identificatienummer, locatiegegevens, een online-identificator, of op een of meer factoren die specifiek zijn voor de fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit van de Betrokkene.

„**Proces**" of „**Verwerking**" betekent elke bewerking of reeks handelingen die worden uitgevoerd met persoonsgegevens van klanten, al dan niet op geautomatiseerde wijze, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, wijzigen, opvragen, raadplegen, gebruiken, openbaar maken, verwijderen, beperken, toegang, verspreiden, combineren, aanpassen, kopiëren, overdragen, wissen en/of vernietigen van persoonsgegevens van klanten.

„**Inbreuk op de beveiliging**" betekent een bevestigde inbreuk op de beveiliging die leidt tot een onbedoelde of onwettige vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking van of toegang tot de verzonden, opgeslagen of anderszins verwerkte persoonsgegevens van de klant.

„**Standaardcontractclausules**" betekent de standaard contractuele vereisten die zijn vastgelegd in de toepasselijke wetgeving inzake gegevensbescherming (standaardcontractclausules van de EU, modelcontractclausules van de RIPD Latin American Data Protection Board, modelcontractclausules van de ASEAN, enz.).

„Derde partij" betekent een andere partij dan de klant of het bedrijf.

De termen „**verwerkingsverantwoordelijke**", „**verwerker**" en „**toezichthoudende autoriteit**" zoals gebruikt in deze gegevensbeschermingsautoriteit zullen de betekenis hebben die eraan wordt toegekend in de toepasselijke wetgeving inzake gegevensbescherming.

Alle andere termen zonder hoofdletters hebben de betekenis die is vastgelegd in de Overeenkomst of de toepasselijke wetgeving inzake gegevensbescherming.

2. Verwerking van persoonsgegevens van klanten

2.1 Doel van de verwerking. Het doel van de gegevensverwerking in het kader van deze gegevensbeschermingsautoriteit is de levering van producten en/of diensten op grond van de overeenkomst. Bijlage 1 beschrijft het onderwerp en de details van de verwerking van persoonsgegevens van klanten.

2.2 Verantwoordelijkheden voor de verwerker en de controller. De partijen erkennen en gaan ermee akkoord dat: (a) het bedrijf een verwerker is van persoonsgegevens van klanten volgens de wetgeving inzake gegevensbescherming; (b) de klant een

beheerder is van de persoonsgegevens van klanten volgens de wetgeving inzake gegevensbescherming; (c) de klant verantwoordelijk is voor het verkrijgen van alle nodige autorisaties en goedkeuringen voor het invoeren, gebruiken, verstrekken, opslaan en verwerken van persoonsgegevens van klanten zodat het bedrijf de producten en/of diensten kan leveren; en (d) elke partij zal voldoen aan de toepasselijke verplichtingen op grond van de wetgeving inzake gegevensbescherming met betrekking tot de verwerking van Persoonlijke gegevens van klanten.

2.3 Amerikaanse wetgeving inzake gegevensbescherming. Voor de doeleinden van de Amerikaanse wetgeving inzake gegevensbescherming (waaronder de CCPA) omvat „verwerkingsverantwoordelijke" „bedrijf"; „verwerker" omvat „dienstverlener"; „Betrokkene" omvat „consument"; en „Persoonsgegevens" omvat „persoonlijke informatie". Het bedrijf is een dienstverlener en de klant is een bedrijf.

2.4 Instructies voor de klant. De klant geeft het bedrijf opdracht om persoonsgegevens van klanten te verwerken: (a) in overeenstemming met de overeenkomst en eventuele toepasselijke supplementen; (b) indien anders nodig om de producten en/of diensten aan de klant te leveren; (c) indien nodig om te voldoen aan de toepasselijke wet- of regelgeving; en (d) om te voldoen aan andere redelijke schriftelijke instructies van de klant, indien dergelijke instructies in overeenstemming zijn met de voorwaarden van de overeenkomst. De klant zal ervoor zorgen dat zijn instructies voor de verwerking van persoonsgegevens van klanten voldoen aan de wetgeving inzake gegevensbescherming. Wat de partijen betreft, is de klant als enige verantwoordelijk voor de nauwkeurigheid, kwaliteit en wettigheid van de persoonlijke gegevens van de klant en de manier waarop de klant de persoonlijke gegevens van de klant heeft verkregen.

2.5 Naleving van de instructies van de klant door het bedrijf. Het bedrijf verwerkt de persoonsgegevens van klanten alleen in overeenstemming met de instructies van de klant en behandelt de persoonlijke gegevens van klanten als vertrouwelijke informatie. Als het bedrijf van mening is of zich ervan bewust wordt dat een van de instructies van de klant in strijd is met de wetgeving inzake gegevensbescherming, zal het bedrijf de klant hiervan binnen een redelijke termijn op de hoogte stellen. Het bedrijf kan persoonsgegevens van klanten verwerken op een andere manier dan in schriftelijke instructies van de klant, indien dit vereist is op grond van de toepasselijke wetgeving waaraan het bedrijf is onderworpen. In deze situatie zal het bedrijf de klant op de hoogte brengen van een dergelijke vereiste voordat het bedrijf de persoonsgegevens van de klant verwerkt, tenzij dit volgens de toepasselijke wetgeving verboden is.

2.6 CCPA-verwerking. Voor zover de verwerking van persoonsgegevens door het bedrijf onderworpen is aan de CCPA, verklaart het bedrijf dat het: (a) de persoonsgegevens van klanten niet zal bewaren, gebruiken of openbaar maken, voor zover dat nodig is om de producten en/of diensten te leveren, om de kwaliteit van de producten en/of diensten op te bouwen of te verbeteren, om beveiligingsincidenten op te sporen, om bescherming te bieden tegen frauduleuze of illegale activiteiten, om subverwerkers te behouden in overeenstemming met deze DPA, of zoals anderszins toegestaan door de CCPA; of (b) persoonlijke gegevens van klanten verkopen of delen.

3. Subverwerkers

3.1 Aanstelling van subverwerkers. De klant geeft het bedrijf hierbij algemene schriftelijke toestemming om externe subverwerkers in te schakelen om beperkte of aanvullende diensten te verlenen in verband met de levering van producten en/of diensten. Op de website van het bedrijf staan subverwerkers die momenteel door het bedrijf zijn ingeschakeld om specifieke verwerkingsactiviteiten met betrekking tot persoonsgegevens van klanten uit te voeren (https://commandalkon.com/sub-processor-list/) en het bedrijf zal de lijst van subverwerkers bijwerken voordat een nieuwe subverwerker wordt ingeschakeld om specifieke verwerking uit te voeren. De klant kan zich aanmelden voor elektronische updates wanneer de lijst van subverwerkers van het bedrijf wordt gewijzigd door een dergelijk verzoek te sturen naar privacy@commandalkon.com. De klant kan bezwaar maken tegen elke subverwerker door dit bezwaar binnen dertig (30) dagen na een update aan het bedrijf mee te delen, en de partijen zullen te goeder trouw te werk gaan om het bezwaar op te lossen. De klant gaat hierbij akkoord met subverwerkingsactiviteiten door huidige subverwerkers die op de website van het bedrijf worden vermeld.

3.2 Beveiliging van de subverwerker. Wanneer het bedrijf zijn verplichtingen uitbesteedt, zal het dat alleen doen door middel van een schriftelijke overeenkomst met de subverwerker die contractuele verplichtingen oplegt die minstens gelijk zijn aan de verplichtingen die op grond van dit addendum aan het bedrijf worden opgelegd. De partijen zijn het erover eens dat kopieën van de overeenkomsten met geautoriseerde subverwerkers die moeten worden verstrekt op grond van de toepasselijke standaardcontractbepalingen, alleen worden verstrekt op schriftelijk verzoek van de klant.

3.3 Aansprakelijkheid. Indien de subverwerker zijn verplichtingen op het gebied van gegevensbescherming op grond van een dergelijke schriftelijke overeenkomst niet nakomt, blijft het bedrijf volledig aansprakelijk jegens de klant voor de uitvoering van de verplichtingen van de subverwerker uit hoofde van een dergelijke overeenkomst.

4. Verantwoordelijkheden op veiligheidsgebied

4.1 Beveiliging van het bedrijf. Het bedrijf zal passende technische en organisatorische maatregelen nemen om de persoonsgegevens van klanten te beschermen („**Informatiebeveiligingsprogramma**"), waarbij rekening wordt gehouden met de stand van de techniek, de kosten van implementatie en de aard, omvang, context en doeleinden van de verwerking, evenals met het risico van verschillende waarschijnlijkheid en ernst voor de rechten en vrijheden van natuurlijke personen. Het bedrijf beheert zichzelf volgens de volgende veiligheidsnormen: NIST 800-171; AWS CIS.

4.2 Beveiliging van klanten. De klant erkent dat de producten en/of diensten bepaalde functies en functionaliteiten bevatten die de klant kan gebruiken en die van invloed zijn op de veiligheid van de persoonsgegevens van de klant die worden verwerkt door het gebruik van de producten en/of diensten door de klant. De klant is verantwoordelijk voor het beoordelen van de informatie die het bedrijf beschikbaar stelt over de gegevensbeveiliging en om onafhankelijk te bepalen of de producten en/of diensten voldoen aan de vereisten en wettelijke verplichtingen van de klant, met

inbegrip van zijn verplichtingen op grond van de toepasselijke wetgeving inzake gegevensbescherming. De klant is verder verantwoordelijk voor het correct configureren van de producten en/of diensten en het gebruik van functies en functionaliteiten die door het bedrijf beschikbaar worden gesteld om de juiste beveiliging te handhaven in het licht van de aard van de persoonsgegevens van klanten die worden verwerkt als gevolg van het gebruik van de producten en/of diensten door de klant. De klant is verantwoordelijk voor het gebruik van de producten en/of diensten en de opslag van alle kopieën van persoonlijke gegevens van klanten buiten de systemen van het bedrijf of de subverwerkers van het bedrijf, met inbegrip van, maar niet beperkt tot, het beveiligen van de inloggegevens, systemen en apparaten van de account, en het bewaren van kopieën van de persoonlijke gegevens van de klant, indien van toepassing.

4.3 Personeel van het bedrijf. Het bedrijf zorgt ervoor dat het personeel dat betrokken is bij de verwerking van persoonsgegevens van klanten op de hoogte wordt gebracht van het vertrouwelijke karakter van de persoonsgegevens van de klant, een passende opleiding heeft gekregen over hun verantwoordelijkheden en onderworpen is aan vertrouwelijkheidsverplichtingen, waarbij dergelijke verplichtingen ook na de beëindiging van de overeenkomst van die persoon met het bedrijf blijven bestaan.

4.4 Veiligheidstests. Het bedrijf zal de doeltreffendheid van het informatiebeveiligingsprogramma testen, beoordelen en evalueren om de veilige verwerking van persoonsgegevens van klanten te garanderen. Het bedrijf zal voldoen aan het informatiebeveiligingsprogramma en verklaart en garandeert dat het informatiebeveiligingsprogramma in overeenstemming is en zal zijn met de toepasselijke wetgeving.

4.5 Effectbeoordelingen. Het bedrijf zal redelijke maatregelen nemen om samen te werken en de klant te helpen bij het uitvoeren van effectbeoordelingen en bijbehorend overleg met elke toezichthoudende autoriteit indien de klant op grond van de wetgeving inzake gegevensbescherming verplicht is dergelijke effectbeoordelingen uit te voeren.

5. Rechten van betrokkenen

5.1 Hulp bij de verplichtingen van de klant. Voor zover de klant bij het gebruik of de ontvangst van de producten en/of diensten niet in staat is om de persoonlijke gegevens van klanten te corrigeren, te wijzigen, te beperken, te blokkeren of te verwijderen, zoals vereist door de wetgeving inzake gegevensbescherming, zal het bedrijf onmiddellijk voldoen aan redelijke verzoeken van de klant om dergelijke acties mogelijk te maken, voor zover het bedrijf dat wettelijk is toegestaan en kan doen. Indien wettelijk toegestaan, is de klant verantwoordelijk voor alle kosten die voortvloeien uit de verlening van dergelijke bijstand door het bedrijf.

5.2 Meldingsverplichtingen. Het bedrijf zal, voor zover wettelijk toegestaan, de klant onmiddellijk op de hoogte stellen als het een verzoek ontvangt van een betrokkene om toegang tot, correctie, wijziging, verwijdering van of bezwaar tegen de verwerking van persoonsgegevens van klanten met betrekking tot een dergelijke persoon. Het bedrijf zal niet reageren op een dergelijk verzoek van de betrokkene met betrekking tot persoonlijke gegevens van klanten zonder voorafgaande schriftelijke toestemming

van de klant, behalve om te bevestigen dat het verzoek betrekking heeft op de klant. Bovendien zal het bedrijf, voor zover wettelijk toegestaan, de klant onmiddellijk op de hoogte stellen als het een verzoek ontvangt om openbaarmaking of correspondentie, kennisgeving of andere communicatie met betrekking tot persoonsgegevens van klanten van wetshandhavingsinstanties, een bevoegde autoriteit of een relevante gegevensbeschermingsautoriteit. Het bedrijf zal de klant passende redelijke medewerking en hulp bieden bij de behandeling van een dergelijk verzoek, voor zover wettelijk toegestaan en voor zover de klant geen toegang heeft tot dergelijke persoonlijke gegevens van klanten door het gebruik of de ontvangst van de producten en/of diensten. Indien wettelijk toegestaan, is de klant verantwoordelijk voor alle kosten die voortvloeien uit de verlening van dergelijke bijstand door het bedrijf.

6. Inbreuk in verband met persoonsgegevens

6.1 Meldingsverplichtingen. Indien het bedrijf kennis neemt van een geverifieerde inbreuk op de beveiliging waarbij persoonsgegevens van klanten betrokken zijn, zal het bedrijf de klant onverwijld en in ieder geval niet later dan tweeënzeventig (72) uur na bevestiging op de hoogte stellen van de inbreuk op de beveiliging. De verplichtingen in dit artikel 6 zijn niet van toepassing op incidenten die worden veroorzaakt door personeel of eindgebruikers van de klant of klant of op mislukte pogingen of activiteiten die de veiligheid van de persoonsgegevens van klanten niet in gevaar brengen, waaronder mislukte inlogpogingen, pings, poortscans, denial-of-service-aanvallen en andere netwerkaanvallen op firewalls of netwerksystemen.

6.2 Wijze van melding. Meldingen van beveiligingsinbreuken, indien van toepassing, worden via e-mail of telefoon naar het contactpunt van de klant gestuurd. Het is de exclusieve verantwoordelijkheid van de klant om ervoor te zorgen dat de contactgegevens op de ondersteuningssystemen van het bedrijf te allen tijde correct zijn. De klant is als enige verantwoordelijk voor het voldoen aan de meldingseisen voor inbreuken die van toepassing zijn op de klant en voor het nakomen van alle meldingsverplichtingen van derden in verband met een inbreuk op de beveiliging van persoonsgegevens.

6.3 Inhoud van de melding. Indien een kennisgeving vereist is, moet deze kennisgeving ten minste:

6.3.1 beschrijf de aard van de inbreuk op de beveiliging, de categorieën en aantallen betrokken betrokkenen, en de categorieën en aantallen persoonsgegevens in kwestie;

6.3.2 geef de naam en contactgegevens door van de relevante contactpersoon van het bedrijf, van wie meer informatie kan worden verkregen;

6.3.3 beschrijf de waarschijnlijke gevolgen van de inbreuk op de beveiliging; en

6.3.4 beschrijf de maatregelen die zijn genomen of voorgesteld om de inbreuk op de beveiliging aan te pakken.

7. Verwijdering of teruggave van persoonsgegevens van klanten

7.1 Verwijderen of terugsturen. Onder voorbehoud van paragraaf 7.3 gaat het bedrijf ermee akkoord om onmiddellijk en in ieder geval binnen dertig (30) dagen na de stopzetting van alle diensten met betrekking tot de verwerking van persoonsgegevens van klanten (de „**stopdatum**") de persoonsgegevens van de klant veilig te verwijderen of, op tijdig schriftelijk verzoek van de klant, een volledig exemplaar van alle persoonsgegevens van de klant terug te sturen aan de klant door middel van een veilige bestandsoverdracht in een formaat dat redelijkerwijs door de klant wordt gevraagd.

7.2 Als de klant en het bedrijf standaardcontractbepalingen hebben gesloten die een schriftelijke verklaring van verwijdering vereisen (zoals clausules 8.5 en 16 van de SCC's van de EU), komen de partijen overeen dat een schriftelijke verklaring alleen wordt verstrekt op schriftelijk verzoek van de klant.

7.3 Definitie van Delete. Ter verduidelijking: „**Verwijderen**" betekent het verwijderen of wissen van persoonlijke gegevens van klanten, zodat deze niet kunnen worden hersteld of gereconstrueerd.

7.4 Records. Het bedrijf mag persoonsgegevens van klanten bewaren voor zover vereist door de toepasselijke wetgeving of zoals voorgeschreven in het schema voor het bewaren van documenten van het bedrijf, op voorwaarde dat het bedrijf de vertrouwelijkheid van al deze persoonsgegevens van klanten garandeert.

8. Auditrechten

8.1 Auditrechten. De klant mag niet meer dan één keer per jaar een onderling overeengekomen derde partij inschakelen om het bedrijf te auditeren, uitsluitend om te voldoen aan de auditvereisten op grond van artikel 28, sectie 3 (h) van de GDPR. Om een audit aan te vragen, moet de klant minstens vier (4) weken voor de voorgestelde auditdatum een gedetailleerd auditplan indienen waarin de voorgestelde omvang, duur en startdatum van de audit worden beschreven. Auditverzoeken moeten worden gestuurd naar privacy@commandalkon.com. Voordat de audit wordt uitgevoerd, moet de auditor een schriftelijke vertrouwelijkheidsovereenkomst opstellen die aanvaardbaar is voor het bedrijf. De audit moet worden uitgevoerd tijdens de reguliere kantooruren, afhankelijk van het beleid van het bedrijf, en mag de bedrijfsactiviteiten van het bedrijf niet op onredelijke wijze beïnvloeden. Alle audits zijn voor rekening en kosten van de klant. Het bedrijf zal samenwerken met elk auditverzoek van de klant of elke bevoegde regelgevende of toezichthoudende autoriteit om na te gaan of het bedrijf voldoet aan zijn verplichtingen uit hoofde van deze DPA door, onder voorbehoud van geheimhoudingsverplichtingen, auditrapporten van derden beschikbaar te stellen, indien beschikbaar, en/of beschrijvingen van beveiligingscontroles en andere informatie die redelijkerwijs door de klant wordt gevraagd met betrekking tot de beveiligingspraktijken en het beleid van het bedrijf.

8.2 Hulp bij de naleving van de regelgeving. Rekening houdend met de aard van de verwerking en de informatie waarover het bedrijf beschikt, zal het bedrijf de klant voldoende redelijke medewerking en bijstand verlenen met betrekking tot de

nalevingsverplichtingen van de klant, zoals beschreven in de artikelen 32-36 van de GDPR.

9. Overdracht van gegevens

9.1 Algemene machtiging. De klant gaat ermee akkoord dat het bedrijf, met inachtneming van paragraaf 9.2, persoonsgegevens van klanten mag opslaan en verwerken in de Verenigde Staten van Amerika en elk ander land waar het bedrijf of een van zijn subverwerkers faciliteiten heeft of anderszins persoonsgegevens verwerkt. Dergelijke overdrachten worden in de eerste plaats geregeld door de certificering van het Data Privacy Framework van het bedrijf of, als alternatief, door de onderling gelieerde standaardcontractbepalingen van het bedrijf. Het bedrijf zal geen persoonlijke gegevens van klanten overdragen of laten overdragen van het ene rechtsgebied naar het andere, tenzij in overeenstemming met de toepasselijke wetgeving, en zal er niet toe leiden dat de klant een wet inzake gegevensbescherming overtreedt.

9.2 Standaardcontractclausules. Voor zover en alleen voor zover het bedrijf persoonsgegevens van klanten uit de Europese Economische Ruimte verwerkt en er standaardcontractclausules nodig zijn, is module twee van de standaardcontractbepalingen van toepassing en wordt deze hierbij opgenomen. Voor de toepassing van de standaardcontractbepalingen is de klant de „gegevensexporteur" en het bedrijf de „gegevensimporteur".

9.3 Brits addendum bij de standaardcontractclausules van de EU. Voor zover, en alleen voor zover het bedrijf persoonsgegevens van klanten uit het Verenigd Koninkrijk verwerkt en er standaardcontractbepalingen vereist zijn, komen de partijen overeen dat het Britse addendum van toepassing is op persoonsgegevens die via de producten en/of diensten vanuit het Verenigd Koninkrijk worden overgedragen, hetzij rechtstreeks, hetzij via verdere overdracht, naar elk land of ontvanger buiten het Verenigd Koninkrijk dat door de bevoegde Britse regelgevende instantie of overheidsinstantie voor het Verenigd Koninkrijk niet wordt erkend als land of ontvanger buiten het Verenigd Koninkrijk dat niet wordt erkend als land of ontvanger buiten het Verenigd Koninkrijk dat niet wordt erkend als land of ontvanger buiten het Verenigd Koninkrijk van bescherming voor persoonlijke gegevens.

9.4 Zwitserse FADP. Voor zover, en alleen voor zover het bedrijf persoonsgegevens van klanten uit Zwitserland verwerkt, zijn de volgende aanvullende vereisten van toepassing voor zover de gegevensoverdrachten uitsluitend onder de FADP vallen of onder zowel de FADP als de EU GDPR vallen: (a) de term „lidstaat" mag niet zodanig worden geïnterpreteerd dat Betrokkenen in Zwitserland worden uitgesloten van de mogelijkheid om een rechtszaak aan te spannen voor hun rechten in hun gewone verblijfplaats (Zwitserland)) in overeenstemming met clausule 18 (c) van de standaardcontractbepalingen; (b) voor zover de gegevensoverdrachten die ten grondslag liggen aan de standaardcontractbepalingen zijn uitsluitend onderworpen aan de FADP, verwijzingen naar de AVG van de EU moeten worden opgevat als verwijzingen naar de FADP; en (c) voor zover de gegevensoverdrachten die ten grondslag liggen aan de standaardcontractclausules onderworpen zijn aan zowel de FADP als de EU-GDPR, moeten de verwijzingen naar de GDPR van de EU worden

opgevat als verwijzingen naar de FADP voor zover de gegevensoverdrachten onderworpen zijn aan de FADP.

9.5 Aanvullende maatregelen. Als aanvulling op de standaardcontractbepalingen verneemt dat een overheidsinstantie (waaronder wetshandhavingsinstanties) toegang wil krijgen tot of een kopie wil krijgen van sommige of alle persoonsgegevens van klanten die door het bedrijf worden verwerkt, hetzij op vrijwillige of verplichte basis, voor doeleinden die verband houden met nationale veiligheidsinformatie, dan zal het bedrijf, tenzij wettelijk verboden of op grond van een dwingende wettelijke verplichting die anders vereist,: 1) de klant op wie de persoonsgegevens van toepassing zijn, hiervan onmiddellijk op de hoogte stellen; 2) de relevante overheidsinstantie die het niet bevoegd is om de persoonlijke gegevens van de klant bekend te maken en moet, tenzij dit wettelijk verboden is, onmiddellijk de klant op de hoogte stellen waarop de persoonsgegevens van de klant van toepassing zijn; 3) de overheidsinstantie ervan op de hoogte brengen dat zij alle verzoeken of verzoeken rechtstreeks moet richten aan de klant op wie de persoonsgegevens van de klant van toepassing zijn; en 4) geen toegang tot de persoonlijke gegevens van de klant verlenen totdat de klant daar schriftelijk toestemming voor heeft gegeven of totdat hij daartoe wettelijk verplicht is. Indien wettelijk verplicht, zal het bedrijf redelijke en wettige inspanningen leveren om een dergelijk verbod of dergelijke dwang aan te vechten. Als het bedrijf gedwongen wordt om de persoonlijke gegevens van de klant te verstrekken, zal het bedrijf de persoonlijke gegevens van klanten alleen bekendmaken voor zover dit wettelijk vereist is in overeenstemming met de toepasselijke wettelijke procedure.

9.6 Wet op het toezicht op de buitenlandse inlichtingendienst. Het bedrijf heeft nog nooit een richtlijn ontvangen op grond van artikel 702 van de Amerikaanse Foreign Intelligence Surveillance Act, gecodificeerd in 50 U.S.C. §1881a („FISA-sectie 702”). Geen enkele rechtbank heeft vastgesteld dat het bedrijf het type entiteit is dat in aanmerking komt voor een procedure die is uitgevaardigd op grond van FISA-sectie 702. Het bedrijf is niet het type aanbieder dat in aanmerking komt voor stroomopwaartse inzameling („bulkinzameling”) overeenkomstig artikel 702 van de FISA, zoals beschreven in het *Schrems* II-besluit.

9.7 Voorrang bij overdracht. In het geval dat diensten onder meer dan één overdrachtsmechanisme vallen, wordt de overdracht van de persoonsgegevens van de klant onderworpen aan één enkel overdrachtsmechanisme in overeenstemming met de volgende rangorde: (i) certificering van het kader voor gegevensbescherming van het bedrijf; (ii) toepasselijke standaardcontractbepalingen (indien vereist volgens de toepasselijke wetgeving inzake gegevensbescherming).

10. Termijn en beëindiging

Termijn van de DPA. Deze gegevensbeschermingsautoriteit wordt van kracht op de datum waarop de overeenkomst volledig is uitgevoerd en blijft, niettegenstaande het verstrijken van de looptijd van een gekocht abonnement, van kracht tot en vervalt automatisch na verwijdering van alle persoonlijke gegevens van klanten zoals beschreven in deze DPA.

11. Niet-naleving; rechtsmiddelen; partijen

11.1 Beperking van aansprakelijkheid. De aansprakelijkheid van het bedrijf voor niet-naleving van de verplichtingen in deze gegevensbeschermingsautoriteit is onderworpen aan de bepaling inzake beperking van aansprakelijkheid in de overeenkomst.

11.2 Partijen bij deze gegevensbeschermingsautoriteit. Niets in de gegevensbeschermingsautoriteit verleent voordelen of rechten aan andere personen of entiteiten dan de partijen bij deze gegevensbeschermingsautoriteit.

12. Algemene voorwaarden

Toepasselijk recht en jurisdictie

12.1 Deze gegevensbeschermingsautoriteit wordt één jaar na de uitgiftedatum geëvalueerd en vervolgens drie jaar daarna, of eerder indien nodig.

12.2 Tenzij vereist op grond van de standaardcontractbepalingen:

12.2.1 de partijen bij dit Addendum onderwerpen zich hierbij aan de keuze van de jurisdictie zoals bepaald in de Overeenkomst met betrekking tot alle geschillen of vorderingen die voortvloeien uit dit Addendum, met inbegrip van geschillen over het bestaan, de geldigheid of de beëindiging ervan; en

12.2.2 dit Addendum en alle niet-contractuele of andere verplichtingen die daaruit voortvloeien of daarmee verband houden, worden beheerst door de wetten van het land of gebied die voor dit doel in de overeenkomst zijn vastgelegd.

Rangorde van voorrang

12.3 In geval van tegenstrijdigheid of inconsistentie tussen dit addendum en de standaardcontractclausules waarbij de standaardcontractclausules vereist zijn, hebben de standaardcontractbepalingen voorrang.

12.4 Onder voorbehoud van paragraaf 12.2, met betrekking tot het onderwerp van dit Addendum, in geval van tegenstrijdigheden tussen de bepalingen van dit Addendum en andere overeenkomsten tussen de partijen, waaronder de overeenkomst en inclusief (tenzij uitdrukkelijk schriftelijk anders overeengekomen, ondertekend namens de partijen) overeenkomsten die zijn gesloten of waarvan wordt beweerd dat ze zijn gesloten na de datum van dit Addendum, hebben de bepalingen van dit Addendum voorrang.

Wijzigingen in de wetgeving inzake gegevensbescherming

12.5 De klant kan:

12.5.1 door het Bedrijf van tijd tot tijd schriftelijk van ten minste dertig (30) kalenderdagen op de hoogte te stellen van eventuele wijzigingen in de standaardcontractbepalingen die vereist zijn als gevolg van een wijziging

of beslissing van een bevoegde autoriteit op grond van die wet inzake gegevensbescherming; en

12.5.2 om het even welke andere wijzigingen op dit addendum voorstellen die de klant redelijkerwijs noodzakelijk acht om te voldoen aan de vereisten van elke wet inzake gegevensbescherming.

12.6 Als de klant op grond van paragraaf 12.5 op de hoogte stelt, zullen de partijen de voorgestelde wijzigingen onmiddellijk bespreken en te goeder trouw onderhandelen om deze of alternatieve varianten, die bedoeld zijn om te voldoen aan de vereisten die zijn geïdentificeerd in de kennisgeving van de klant, zo snel als redelijkerwijs mogelijk is, overeen te komen en te implementeren.

Ontslagvergoeding

12.7 Mocht een bepaling van dit Addendum ongeldig of niet-afdwingbaar zijn, dan blijft de rest van dit Addendum geldig en van kracht. De ongeldige of niet-afdwingbare bepaling wordt ofwel: (i) zo nodig gewijzigd om de geldigheid en afdwingbaarheid ervan te waarborgen, waarbij de bedoelingen van de partijen zo goed mogelijk worden bewaard, of, indien dit niet mogelijk is; (ii) zo uitgelegd alsof het ongeldige of niet-afdwingbare deel er nooit in was opgenomen.

Bijlage I — Details van de gegevensverwerking

Gegevensexporteur (verwerkingsverantwoordelijke): klant zoals geïdentificeerd in de overeenkomst.

Gegevensimporteur (verwerker): Bedrijf zoals geïdentificeerd in de overeenkomst.

Onderwerp: Het onderwerp van de gegevensverwerking in het kader van deze gegevensbeschermingsautoriteit zijn de persoonsgegevens van de klant.

Duur van de verwerking: De duur van de overeenkomst plus de periode totdat het bedrijf alle persoonsgegevens van klanten verwijdert in overeenstemming met deze DPA.

Doel: Het doel van de gegevensverwerking is de levering van producten en/of diensten aan de klant.

Aard van de verwerking: De aard van de gegevensverwerking is bedoeld voor de levering van de producten en/of diensten zoals beschreven in de overeenkomst.

Categorieën van betrokkenen: Klanten, werknemers en werknemers van filialen, klanten en zakenpartners van klanten.

Soorten persoonsgegevens: de klant mag bepaalde persoonlijke gegevens van klanten uploaden, indienen of anderszins verstrekken aan de producten en/of diensten, waarvan de omvang doorgaans naar eigen goeddunken wordt bepaald en beheerd, en kan bestaan uit contactgegevens; informatie over interactie tussen website, product en service; adressen; geboortedatum; geboorteplaats; e-mailadressen; namen; geslacht; titel; telefoonnummers; rijbewijsnummer; handtekening; werknemersnummer; geolocatiegegevens; loontarief; gebruikersnaam; wachtwoord; prestatie informatie; kwalificaties en beperkingen; informatie over het apparaat.

Gevoelige gegevens overgedragen: niets.

Frequentie van de overdracht: Doorlopend indien nodig voor de levering van de producten en/of diensten.

Overdrachten naar subverwerkers: zoals beschreven in de lijst van subverwerkers van het bedrijf, die beschikbaar is op https://commandalkon.com/sub-processor-list/.

Bevoegde toezichthoudende autoriteit: zoals bepaald door de toepasselijke wetgeving inzake gegevensbescherming of, in volgorde van werking, 1) in overeenstemming met de voorwaarden van de overeenkomst of 2) de Nederlandse Gegevensbeschermingsautoriteit.

Bewaring: In overeenstemming met de overeenkomst en deze gegevensbeschermingsautoriteit.

Technische en organisatorische maatregelen: De technische en organisatorische beveiligingsmaatregelen die door de gegevensimporteur zijn geïmplementeerd, worden beschreven in paragraaf 4.1 van de DPA. Aanvullende informatie is op aanvraag beschikbaar.