Privacyplan

c.k.v. ODIK
p/a Roggeakker 13
3773 AA Barneveld

Inleiding

De General Data Protection Regulation (GDPR) is een nieuwe wereldwijde standaard wet op het gebied van privacy en bescherming van persoonsgegevens. De GDPR is sinds april 2016 in werking getreden. In Nederland is de GDPR van toepassing vanaf 25 mei 2018.

De GDPR wordt in Nederland aangeduid als de Algemene Verordening Gegevensbescherming (AVG). De AVG vervangt de huidige Nederlandse Wet Bescherming Persoonsgegevens (WBP) en is bedoeld om privacyrechten van personen te waarborgen en beveiligen. De AVG schrijft voor hoe je als organisatie persoonsgegevens moet beheren en beveiligen.

ODIK beheert en verwerkt verschillende soorten persoonsgegevens met verschillende doeleinden. Het gaat daarbij om persoonsgegevens van volwassen leden, jeugdleden, vrijwilligers en ouders van leden. In dit plan is omschreven hoe we deze gegevens verwerken, beheren en beveiligen. Ook is vastgelegd hoe we omgaan met een eventueel datalek.

Omdat ODIK een vereniging is, minder dan 250 personen in dienst heeft en de verwerkte gegevens geen hoog risicoprofiel hebben is geen gegevensbeschermingseffectbeoordeling (DPIA) uitgevoerd. Ook is geen functionaris gegevensbescherming aangesteld. De verantwoordelijkheid voor het opstellen, bijhouden en bekend maken van het privacybeleid berust bij het bestuur, waarbinnen de voorzitter aanspreekpunt is op dit thema.

Het bestuur zal regelmatig de leden informeren over het belang van privacybescherming en instructie geven hoe we samen zo veilig mogelijk kunnen omgaan met persoonsgegevens.

Bestuur c.k.v. ODIK Barneveld, mei 2018

Bijlage A: Verwerkingsregister ODIK
Bijlage B: Fotografiebeleid ODIK
Bijlage C: Verwerkersovereenkomst Mailchimp

Visie op privacy en bescherming persoonsgegevens

ODIK gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. ODIK houdt zich hierbij aan de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

Grondslag en doelbinding
ODIK zorgt ervoor dat persoonsgegevens alleen voor bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

Dataminimalisatie
ODIK verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. ODIK streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bewaartermijn
Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

Integriteit en vertrouwelijkheid
ODIK gaat zorgvuldig om met persoonsgegevens, behandelt deze vertrouwelijk en zorgt voor passende beveiliging van persoonsgegevens.

Delen met derden
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt ODIK afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet.

Subsidiariteit
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken personen zoveel mogelijk beperkt.

Proportionaliteit
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.

Rechten van betrokkenen
ODIK honoreert alle rechten van betrokkenen.

Wat zijn persoonsgegevens precies?

Gegevens zijn persoonsgegevens als ze informatie bevatten over een natuurlijke persoon; en die persoon door de gegevens identificeerbaar is. Het kan daarbij gaan om informatie in de vorm van tekst, beeld en/of geluid. Er zijn veel verschillende soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd. Hieronder volgt een (niet-uitputtende) lijst met persoonsgegevens ter indicatie wat we in dit plan verstaan onder deze term.

Gewone persoonsgegevens:

- naam;
- geboortedatum;
- geslacht;
- adres;
- postcode;
- woonplaats;
- telefoonnummer;
- e-mailadres;
- ip-adres;

Bijzondere persoonsgegevens:

- godsdienst of levensovertuiging;
- ras;
- politieke voorkeur;
- gezondheid;
- seksuele leven;
- lidmaatschap van een vakbond;
- strafrechtelijk verleden;
- vingerafdrukken;
- Burgerservicenummer (BSN);
- (pas)foto’s.

Welke gegevens verwerkt ODIK en waarom?

Binnen ODIK gaan veel persoonsgegevens om. Van geboortedata en NAW-gegevens van leden tot foto's van spelers en toeschouwers. Het verwerken van zulke persoonsgegevens is voor ODIK noodzakelijk om te kunnen functioneren als vereniging. Er dient contributie geind te worden, zonder persoonsgegevens kunnen leden niet geinformeerd over wie er in welk team zit, wanneer traint of moet rijden naar een uitwedstrijd. Ook kan er zonder gegevens niet deelgenomen worden aan competitiewedstrijden. Leden geven toestemming voor het verwerken van hun persoonsgegevens bij het aangaan van een lidmaatschap. Voor jeugdleden geldt dat ouders deze toestemming geven. Hieronder lichten we toe welke gegevens we structureel verwerken, met welk doel, op welke grondslag en waar deze gegevens staan.

Persoonsgegevens volwassen leden (senioren)

Persoonsgegeven	**Doel**	**Opslag**	**Grondslag**
Naam	Deelname aan competitie	Sportlink, website	Toestemming + benodigd voor uitvoering van de overeenkomst
Adres	Informeren	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
Postcode	Informeren	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
Woonplaats	Informeren	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
Geboortedatum	Indeling in team + deelname aan competitie	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
E-mailadres	Indien jeugdleden een eigen e-mailadres hebben	Sportlink, Mailchimp	Toestemming + benodigd voor uitvoering van de overeenkomst
Telefoonnummer	Informeren	Sportlink	Toestemming + benodigd voor uitvoering van overeenkomst
Rekeningnummer	Afschrijven van	Sportlink	Toestemming +

	contributie		benodigd voor uitvoering van de overeenkomst
Pasfoto	Identificatie op digitale spelerskaart	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst

Persoonsgegevens jeugdleden (<18 jaar)

Persoonsgegeven	**Doel**	**Opslag**	**Grondslag**
Naam	Deelname aan competitie	Sportlink, website	Toestemming + benodigd voor uitvoering van de overeenkomst
Adres	Informeren, verjaardagskaart, thuisbrengen jeugdleden na wedstrijd	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
Postcode	Informeren, verjaardagskaart	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
Woonplaats	Informeren, verjaardagskaart, thuisbrengen jeugdleden na wedstrijd	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
Geboortedatum	Indeling in team + deelname aan competitie	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
E-mailadres (indien beschikbaar, doorgaans bij oudere jeugdleden)	Informeren	Sportlink, Mailchimp	Toestemming + benodigd voor uitvoering van de overeenkomst
Telefoonnummer (indien beschikbaar, doorgaans bij oudere jeugdleden)	Informeren	Sportlink, Whatsapp	Toestemming + benodigd voor uitvoering van overeenkomst

Pasfoto	Identificatie op digitale spelerskaart	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst

Persoonsgegevens ouders jeugdleden

Persoonsgegeven	**Doel**	**Opslag**	**Grondslag**
Naam	Afschrijven contributie	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
Adres	Informeren	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
Postcode	Informeren	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
Woonplaats	Informeren	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst
E-mailadres	Informeren	Sportlink, Mailchimp	Toestemming + benodigd voor uitvoering van de overeenkomst
Telefoonnummer	Informeren	Sportlink, Whatsapp	Toestemming + benodigd voor uitvoering van overeenkomst
Rekeningnummer	Afschrijven van contributie	Sportlink	Toestemming + benodigd voor uitvoering van de overeenkomst

Persoonsgegevens die we incidenteel verwerken

Naast de gegevens die we structureel verwerken omdat ze noodzakelijk zijn voor het functioneren van de vereniging en het uitvoeren van de overeenkomst met de leden, verwerken we ook incidenteel persoonsgegevens voor overige doeleinden. Het gaat hierbij

om foto’s die gemaakt worden van wedstrijden, trainingen en activiteiten binnen ODIK. Ze geven een inkijkje in het verenigingsleven en zorgen voor onderlinge binding. In bijlage B is apart ons beleid op dit gebied beschreven.

Hoe beheren we persoonsgegevens?

ODIK zoekt in het beheer van persoonsgegevens naar een balans tussen de bescherming van de privacyrechten van haar leden en het soepel kunnen functioneren als vereniging. Daarbij geldt dat we extra aandacht schenken aan privacybescherming van leden onder de 18 jaar en bijzondere persoonsgegevens zoals foto's.

Hoe gebruiken we persoonsgegevens?

Sportlink

- ODIK maakt gebruik van Sportlink als verenigingsadministratie. Dit is een verplichting vanuit het KNKV. Elk spelend lid heeft een eigen digitale spelerskaart in Sportlink. Deze spelerskaart is benodigd om deel te nemen aan competitiewedstrijden en wordt voor aanvang digitaal gecontroleerd door de scheidsrechter van de betreffende wedstrijd.

Mailings

- ODIK verstuurt tweewekelijks nieuwsbrieven naar leden. Hierin informeren we over allerhande verenigingszaken die spelen. Voor deze mailings maken we gebruik van Mailchimp. ODIK heeft uitsluitend e-mailadressen van leden en ouders gedeeld met Mailchimp. In elke mailing hebben ontvangers de mogelijkheid om zich uit te schrijven.

WhatsaAppgroepen

- Voor elk team wordt jaarlijks een WhatsApp-groep aangemaakt. Bij jeugdteams (t/m C) gaat het om groepen met ouders, bij oudere leden om de leden zelf. In deze groepen wordt informatie gedeeld over o.a. wedstrijden, vertrektijden, activiteiten, wasafspraken etc.

Website

- ODIK deelt jaarlijks teams in en maakt deze indelingen bekend via de website. Ook wordt er een teamfoto van elk team gemaakt, zodat voor iedereen duidelijk is wie er in welk team speelt.
- Bij jeugdteams wordt voor uitwedstrijden een rijschema gemaakt, zodat ouders weten wanneer ze aan de beurt zijn om hun kind en teamgenoten te vervoeren. Dit rijschema wordt gepubliceerd op de website.
- ODIK kent diverse commissies die verantwoordelijk zijn voor uitvoering van verenigingstaken. Contactpersonen van deze commissies worden vermeld op de website met naam, e-mailadres en soms ook telefoonnummer zodat leden hen kunnen bereiken. Contactpersonen bepalen zelf welke informatie ze vrijgeven.
- ODIK maakt gebruik van Google Analytics om bij te houden hoe gebruikers de website gebruiken.

Social media

- ODIK publiceert op Twitter, Facebook en Instagram foto's van activiteiten en wedstrijden. Op deze foto's zijn soms leden herkenbaar in beeld. Het delen van deze foto's achten we noodzakelijk voor de onderlinge betrokkenheid en uitstraling van de vereniging. Indien leden hier om privacyredenen bezwaar tegen hebben, kunnen ze

dit kenbaar maken aan ODIK. We zullen we de betreffende uiting in dat geval binnen dertig (30) werkdagen verwijderen van onze website en sociale media.

Hoe beheren we persoonsgegevens?

Binnen ODIK is het secretariaat belast met en verantwoordelijk voor de verwerking van persoonsgegevens. De secretaris delegeert de verwerking van persoonsgegevens naar verschillende personen en commissies binnen de vereniging. Het gaat hierbij onder andere om:

- Administratief vrijwilliger: die mutaties in gegevens verwerkt in Sportlink.
- Penningmeester: die contributies incasseert.
- Wedstrijdsecretariaat, TC & JTC: die samen teamindelingen maken.
- Jeugdtrainers: die Whatsapp-groepen samenstellen
- PR-commissie: die mailings verzorgen en de website bijhouden.

We hanteren hierbij het principe dat we niet meer persoonsgegevens delen dan noodzakelijk is voor het uitoefenen van een taak. De PR-commissie beschikt bijvoorbeeld alleen over e-mailadressen van leden, jeugdtrainers krijgen telefoonnummers van ouders, maar geen rekeningnummers etc.

Hoe lang bewaren we persoonsgegevens?

ODIK bewaart persoonsgegevens zolang iemand lid is van de vereniging. Na uitschrijving worden de gegevens binnen dertig (30) dagen verwijderd uit Sportlink en Mailchimp. Op de website worden gegevens met ingang van het nieuwe seizoen verwijderd.

Met wie delen we persoonsgegevens?

- ODIK deelt alle in hoofdstuk 2 omschreven persoonsgegevens met Sportlink. Sportlink heeft alle aspecten van de verwerkersovereenkomst verwerkt in haar algemene voorwaarden, die we geaccepteerd hebben. De voorwaarden van Sportlink zijn hier in te zien.
- ODIK deelt e-mailadressen van leden met Mailchimp. Hiervoor is met Mailchimp een verwerkersovereenkomst afgesloten. Zie bijlage C.
- ODIK deelt gegevens van websitebezoekers, waaronder ip-adressen, met Google. De verkregen informatie wordt overgebracht naar en door Google opgeslagen op servers in de Verenigde Staten. Lees het privacybeleid van Google voor meer informatie. Je treft ook het privacybeleid van Google Analytics hier aan. Google gebruikt deze informatie om bij te houden hoe onze website gebruikt wordt, om rapporten over de website te kunnen verstrekken en om haar adverteerders informatie over de effectiviteit van hun campagnes te kunnen bieden. Google kan deze informatie aan derden verschaffen indien Google hiertoe wettelijk wordt verplicht, of voor zover deze derden de informatie namens Google verwerken. ODIK heeft hier geen invloed op. ODIK heeft Google geen toestemming gegeven om via ODIK verkregen Analytics-informatie te gebruiken voor andere Google-diensten.

Welk proces hanteren we voor inzage, verbetering, verwijdering etc. van persoonsgegevens?

Leden, ouders van jeugdleden en vrijwilligers kunnen te allen tijde opvragen welke persoonsgegevens ODIK van hem of haar bezit. ODIK zal een verzoek hiertoe binnen dertig (30) werkdagen afhandelen en de betreffende persoon per e-mail een gestructureerd overzicht sturen met de betreffende gegevens, zodat de gebruiker deze eventueel kan verplaatsen naar een andere locatie of dienstverlener.

Leden, ouders van jeugdleden en vrijwilligers hebben tevens het recht om gegevens te verwijderen of te corrigeren, om te verzoeken de gegevens niet langer te gebruiken, om bezwaar te maken tegen informerende mails/brieven en de toestemming in te trekken voor bepaalde toepassingen van hun gegevens. ODIK zal een verzoek hiertoe binnen dertig (30) werkdagen afhandelen en de betreffende persoon per e-mail een bevestiging sturen van de uitgevoerde actie. Het verwijderen van gegevens of intrekken van toestemming kan gevolgen hebben voor de mogelijkheid om deel te nemen aan het verenigingsleven of competitiewedstrijden.

Hoe is dataportabiliteit geregeld?

Indien een lid wenst over te stappen naar een andere korfbalvereniging, dan wordt binnen Sportlink een overschrijving geregeld. De gegevens gaan daarmee uit onze administratie over naar de administratie van de nieuwe vereniging. Desgewenst kan ook een export gemaakt worden van gegevens in Sportlink.

Hoe beveiligen we persoonsgegevens?

ODIK vindt het belangrijk om persoonsgegevens van leden, ouders van leden en vrijwilligers adequaat te beschermen. Omdat we een vereniging zijn, zijn onze mogelijkheden hiertoe wel beperkter dan die van bedrijven. Hieronder beschrijven we hoe we bij ODIK persoonsgegevens beschermen en omgaan met eventuele datalekken.

Hoe beveiligen we persoonsgegevens?

Technische maatregelen:

- ODIK is een vereniging zonder eigen pand met ICT-faciliteiten of medewerkers die centraal gegevens verwerken. Gegevensverwerking gebeurt thuis door vrijwilligers. ODIK heeft geen invloed op technische beveiliging van devices waarop dit gebeurt, maar stimuleert vrijwilligers die werken met persoonsgegevens wel om in ieder geval een firewall en virusscanner te installeren.

Organisatorische maatregelen:

- ODIK verstrekt vrijwilligers die werken met persoonsgegevens een document met richtlijnen die privacybewustzijn stimuleren en bescherming van persoonsgegevens borgen. Het gaat hierbij onder meer om het gebruiken van unieke en sterke wachtwoorden, het regelmatig veranderen van wachtwoorden en het afschermen van persoonsgegevens van ODIK-leden van andere gegevens op de devices.
- ODIK verstrekt vrijwilligers die werken met persoonsgegevens niet meer gegevens dan noodzakelijk zijn voor het uitoefenen van hun taak.
- ODIK besteedt meerdere keren per jaar aandacht aan privacy en het belang van gegevensbescherming via haar website, nieuwsbrief en sociale media.

Hoe gaan we om met datalekken?

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt ODIK dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan het AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt ODIK dit aan de betrokkenen in eenvoudige en duidelijke taal.

Bijlage B

Gegevensverwerking m.b.t. fotografie

Volgens de AVG moet elke gegevensverwerking moet volgens de Verordening “gerechtvaardigd” zijn. De verwerking is gerechtvaardigd wanneer het doel van de verwerking is gebaseerd op één of meer van de zes rechtsgrondslagen die in de verordening worden gegeven. Voor een sportvereniging als ODIK zijn in het bijzonder 2 grondslagen relevant:

1. Persoonsgegevens mogen worden verwerkt als de betrokkene hiervoor **toestemming** heeft gegeven.
2. Persoonsgegevens mogen worden verwerkt als dit noodzakelijk is voor de **behartiging van het gerechtvaardigde belang** van de vereniging, mits de belangen, rechten en vrijheden van de betrokkene(n) niet zwaarder wegen.

ad 1
Door het geven van toestemming door betrokkene mag de vereniging persoonsgegevens verwerken. Denk daarbij aan het publiceren van (team)foto’s met de namen van spelers op de website van ODIK.
Als (ouders van) leden daarvoor géén toestemming verlenen, mogen dat soort gegevens dus niet meer gepubliceerd / verwerkt worden. ODIK ziet de inschrijving als lid als toestemming om deze gegevens te verwerken op onder meer spelerskaarten en op de website.

Als er zwaarwegende argumenten zijn om die toestemming niet te verlenen, kunnen leden van 18 jaar en ouder en de wettelijke vertegenwoordigers van leden jonger dan 18 jaar dat bij het bestuur kenbaar maken via info@odik.nl. Let wel; die mogelijkheid geldt niet voor de persoonsgegevens op de digitale spelerskaart! Want daarmee komen we op de 2e grondslag:

ad 2
Het verwerken van persoonsgegevens via digitale spelerskaarten is voor de vereniging noodzakelijk om de wedstrijdadministratie te kunnen voeren. Scheidsrechters controleren aan de hand van de namen en foto’s op spelerskaarten welke spelers aan een wedstrijd deelnemen en deze gegevens worden op hun speelgerechtigheid getoetst door het KNKV. Daarmee is sprake van het “behartigen van een gerechtvaardigd belang” van de vereniging. Leden die nochtans bezwaar hebben tegen verwerking van deze gegevens kunnen dus niet meer aan de competitie deelnemen en dus geen spelend lid meer zijn. Ook dat kan worden gemeld bij het bestuur, uiterlijk op 1 juni i.v.m. de teamindelingen en de door de vereniging aan het KNKV te betalen contributie.

Als gerechtvaardigd belang zien we tevens het maken van foto’s van trainingen, wedstrijden en andere activiteiten die ODIK ontplooit. Foto’s hiervan dragen bij aan de onderlinge betrokkenheid binnen de verenigingen en geven potentiële leden een beeld van de vereniging en het verenigingsleven. We beseffen dat het maken van foto’s een mogelijke inbreuk is op de privacy van leden en bezoekers, in het bijzonder van zij die jonger zijn dan 18 jaar. Desalniettemin achtten we het belang van de vereniging groter en het praktisch ondoenlijk om iedereen vooraf toestemming te vragen om foto’s te maken. Daarom informeren we bezoekers van ons complex op de website en via een bordje bij de entree van het complex dat er foto’s op het complex gemaakt kunnen worden. Fotografen die foto’s maken voor de website van ODIK opereren onder de verantwoordelijkheid van de vereniging. Het bestuur ziet toe dat ze bij het uitoefenen van hun taak handelen in lijn met

het privacybeleid van de vereniging en de privacy van leden en bezoekers niet buiten proportie aantasten.

Als er zwaarwegende argumenten zijn van leden of bezoekers om niet herkenbaar in beeld te komen kunnen zij die bij het bestuur kenbaar maken via info@odik.nl. Het bestuur zal er in dat geval zorg voor dragen dat de beelden verwijderd worden van de website en social media van ODIK.

Bijlage C

Customer EU Data Processing Addendum

This Data Processing Addendum ("DPA"), forms part of the Agreement between The Rocket Science Group LLC d/b/a MailChimp ("MailChimp") and ODIK ("Customer") and shall be effective on the date both parties execute this DPA (Effective Date"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

"Affiliate" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"Agreement" means MailChimp's Terms of Use, which govern the provision of the Services to Customer, as such terms may be updated by MailChimp from time to time.

"Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly.

"Customer Data" means any Personal Data that MailChimp processes on behalf of Customer as a Data Processor in the course of providing Services, as more particularly described in this DPA.

"Data Protection Laws" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

"Data Controller" means an entity that determines the purposes and means of the processing of Personal Data.

"Data Processor" means an entity that processes Personal Data on behalf of a Data Controller.

"EU Data Protection Law" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("Directive") and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

"EEA" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

"Group" means any and all Affiliates that are part of an entity's corporate group.

"Personal Data" means any information relating to an identified or identifiable natural person.

"Privacy Shield" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

"Privacy Shield Principles" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

"Processing" has the meaning given to it in the GDPR and "process", "processes" and "processed" shall be interpreted accordingly.

"Security Incident" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

"Services" means any product or service provided by MailChimp to Customer pursuant to the Agreement.

"Sub-processor" means any Data Processor engaged by MailChimp or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or members of the MailChimp Group.

2. Relationship with the Agreement

2.1 The parties agree that DPA shall replace any existing DPA the parties may have previously entered into in connection with the Services.

2.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

2.3 Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

2.4 Any claims against MailChimp or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. Customer further agrees that any regulatory penalties incurred by MailChimp in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce MailChimp's liability under the Agreement as if it were liability to the Customer under the Agreement.

2.5 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

2.6 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

3. Scope and Applicability of this DPA

3.1 This DPA applies where and only to the extent that MailChimp processes Customer Data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.

3.2 Part A (being Section 4 – 8 (inclusive) of this DPA, as well as Annexes A and B of this DPA) shall apply to the processing of Customer Data within the scope of this DPA from the Effective Date.

3.3 Part B (being Sections 9-12 (inclusive) of this DPA) shall apply to the processing of Customer Data within the scope of the DPA from and including 25th May 2018. For the avoidance of doubt, Part B shall apply in addition to, and not in substitution for, the terms in Part A.

Part A: General Data Protection Obligations

4. Roles and Scope of Processing

4.1 Role of the Parties. As between MailChimp and Customer, Customer is the Data Controller of Customer Data, and MailChimp shall process Customer Data only as a Data Processor acting on behalf of Customer.

4.2. Customer Processing of Customer Data. Customer agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to MailChimp; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for MailChimp to process Customer Data and provide the Services pursuant to the Agreement and this DPA.

4.3 MailChimp Processing of Customer Data. MailChimp shall process Customer Data only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to MailChimp in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and MailChimp.

4.4 Details of Data Processing

(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

(b) Duration: As between MailChimp and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(c) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of MailChimp's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

(d) Nature of the processing: MailChimp provides an email service, automation and marketing platform and other related services, as described in the Agreement.

(e) Categories of data subjects: Any individual accessing and/or using the Services through the Customer's account ("Users"); and any individual: (i) whose email address is included in the Customer's Distribution List; (ii) whose information is stored on or collected via the Services, or (iii) to whom Users send emails or otherwise engage or communicate with via the Services (collectively, "Subscribers").

(f) Types of Customer Data:

- **(i) Customer and Users: identification and contact data (name, address, title, contact details, username); financial information (credit card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility);**
- **(ii) Subscribers: identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address), personal interests or preferences (including purchase history, marketing preferences and publically available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).**

4.5 Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that MailChimp shall have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws, MailChimp is the Data Controller of such data and accordingly shall process such data in accordance with the MailChimp Privacy Policy and Data Protection Laws.

4.6 Tracking Technologies. Customer acknowledges that in connection with the performance of the Services, MailChimp employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("Tracking Technologies"). Customer shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable MailChimp to deploy Tracking Technologies lawfully on, and collect data from, the devices of Subscribers (defined below) in accordance with and as described in theMailChimp Cookie Statement.

5. Subprocessing

5.1 Authorized Sub-processors. Customer agrees that MailChimp may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by MailChimp and authorized by Customer are listed in Annex A.

5.2 Sub-processor Obligations. MailChimp shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause MailChimp to breach any of its obligations under this DPA.

6. Security

6.1 Security Measures. MailChimp shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with MailChimp's security standards described in Annex B ("Security Measures").

6.2 Updates to Security Measures. Customer is responsible for reviewing the information made available by MailChimp relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that MailChimp may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

6.3 Customer Responsibilities. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

7. Security Reports and Audits

7.1 Customer acknowledges that MailChimp is regularly audited against SSAE 16 and PCI standards by independent third party auditors and internal auditors, respectively. Upon request, MailChimp shall supply (on a confidential basis) a summary copy of its audit report(s) ("Report") to Customer, so that Customer can verify MailChimp's compliance with the audit standards against which it has been assessed, and this DPA.

7.2 MailChimp shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm MailChimp's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

8. International Transfers

8.1 Data center locations. MailChimp may transfer and process Customer Data anywhere in the world where MailChimp, its Affiliates or its Sub-processors maintain data processing operations. MailChimp shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

8.2 Privacy Shield. To the extent that MailChimp processes any Customer Data protected by EU Data Protection Law under the Agreement and/or that originates from the EEA, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that MailChimp shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data by virtue of having self-certified its compliance with Privacy Shield. MailChimp agrees to protect such Personal Data in accordance with the requirements of the Privacy Shield Principles. If MailChimp is unable to comply with this requirement, MailChimp shall inform Customer.

8.3 Alternative Transfer Mechanism. The parties agree that the data export solution identified in Section 8.2 shall not apply if and to the extent that MailChimp adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under EU Data Protection Laws) outside of the EEA ("Alternative Transfer Mechanism"), in which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Personal Data is transferred).

Part B: GDPR Obligations from 25 May 2018

9. Additional Security

9.1 Confidentiality of processing. MailChimp shall ensure that any person who is authorized by MailChimp to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

9.2 Security Incident Response. Upon becoming aware of a Security Incident, MailChimp shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

10. Changes to Sub-processors

10.1 MailChimp shall (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which email shall suffice) if it adds or removes Sub-processors at least 10 days prior to any such changes.

10.2 Customer may object in writing to MailChimp's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

11. Return or Deletion of Data

11.1 Upon termination or expiration of the Agreement, MailChimp shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, save that this requirement shall not apply to the extent MailChimp is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data MailChimp shall securely isolate and protect from any further processing, except to the extent required by applicable law.

12. Cooperation

12.1 The Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, MailChimp shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to MailChimp, MailChimp shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If MailChimp is required to respond to such a request, MailChimp shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

12.2 If a law enforcement agency sends MailChimp a demand for Customer Data (for example, through a subpoena or court order), MailChimp shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, MailChimp may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then MailChimp shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless MailChimp is legally prohibited from doing so.

12.3 To the extent MailChimp is required under EU Data Protection Law, MailChimp shall (at Customer's expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative:

The Rocket Science Group LLC d/b/a MailChimp

By:

Name: Daniel Kurzius

Title: CCO/Co-founder

Date: May 19, 2018

ODIK

Name: Rick Borkent

Title: Voorzitter

Date: May 19, 2018

Annex A - List of MailChimp Sub-processors

MailChimp uses its Affiliates and a range of third party Sub-processors to assist it in providing the Services (as described in the Agreement). These Sub-processors set out below provide cloud hosting and storage services; content delivery and review services; assist in providing customer support; as well as incident tracking, response, diagnosis and resolution services.

Entity Name	Corporate Location
Akamai	Massachusetts, USA
Amazon	Washington, USA
E-Hawk	New York, USA
El Camino	California, USA
FullContact	Colorado, USA
Google	California, USA
Neustar	Virginia, USA
R.R. Donnelley	Illinois, USA
Slack	California, USA
TaskUs	California, USA
Zendesk	California, USA

Annex B – Security Measures

The Security Measures applicable to the Services are described here https://mailchimp.com/about/security/ (as updated from time to time in accordance with Section 6.2 of this DPA).

stomer EU Data Processing Addendum

This Data Processing Addendum ("**DPA**"), forms part of the Agreement between The Rocket Science Group LLC d/b/a MailChimp ("**MailChimp**") and ODIK ("**Customer**") and shall be effective on the date both

parties execute this DPA (**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.
"**Agreement**" means MailChimp's Terms of Use, which govern the provision of the Services to Customer, as such terms may be updated by MailChimp from time to time.
"**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" shall be construed accordingly.
"**Customer Data**" means any Personal Data that MailChimp processes on behalf of Customer as a Data Processor in the course of providing Services, as more particularly described in this DPA.
"**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.
"**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.
"**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.
"**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**") and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).
"**EEA**" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.
"**Group**" means any and all Affiliates that are part of an entity's corporate group.
"**Personal Data**" means any information relating to an identified or identifiable natural person.
"**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.
"**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).
"**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.
"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.
"**Services**" means any product or service provided by MailChimp to Customer pursuant to the Agreement.
"**Sub-processor**" means any Data Processor engaged by MailChimp or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or members of the MailChimp Group.

2. Relationship with the Agreement

2.1 The parties agree that DPA shall replace any existing DPA the parties may have previously entered into in connection with the Services.
2.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.
2.3 Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

2.4 Any claims against MailChimp or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. Customer further agrees that any regulatory penalties incurred by MailChimp in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce MailChimp's liability under the Agreement as if it were liability to the Customer under the Agreement.
2.5 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.
2.6 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

3. Scope and Applicability of this DPA

3.1 This DPA applies where and only to the extent that MailChimp processes Customer Data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.
3.2 Part A (being Section 4 – 8 (inclusive) of this DPA, as well as Annexes A and B of this DPA) shall apply to the processing of Customer Data within the scope of this DPA from the Effective Date.
3.3 Part B (being Sections 9-12 (inclusive) of this DPA) shall apply to the processing of Customer Data within the scope of the DPA from and including 25th May 2018. For the avoidance of doubt, Part B shall apply in addition to, and not in substitution for, the terms in Part A.

Part A: General Data Protection Obligations

4. Roles and Scope of Processing

4.1 **Role of the Parties**. As between MailChimp and Customer, Customer is the Data Controller of Customer Data, and MailChimp shall process Customer Data only as a Data Processor acting on behalf of Customer.
4.2. **Customer Processing of Customer Data**. Customer agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to MailChimp; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for MailChimp to process Customer Data and provide the Services pursuant to the Agreement and this DPA.
4.3 **MailChimp Processing of Customer Data**. MailChimp shall process Customer Data only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to MailChimp in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and MailChimp.
4.4 **Details of Data Processing**
(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Data.
(b) Duration: As between MailChimp and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.
(c) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of MailChimp's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.
(d) Nature of the processing: MailChimp provides an email service, automation and marketing platform and other related services, as described in the Agreement.
(e) Categories of data subjects: Any individual accessing and/or using the Services through the Customer's account ("**Users**"); and any individual: (i) whose email address is included in the Customer's Distribution List; (ii) whose information is stored on or collected via the Services, or (iii) to whom Users send emails or otherwise engage or communicate with via the Services (collectively, "**Subscribers**").
(f) Types of Customer Data:

- (i) Customer and Users: identification and contact data (name, address, title, contact details, username); financial information (credit card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility);
- (ii) Subscribers: identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address), personal interests or preferences (including purchase history, marketing preferences and publically available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).

4.5 Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that MailChimp shall have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws, MailChimp is the Data Controller of such data and accordingly shall process such data in accordance with the MailChimp Privacy Policy and Data Protection Laws.

4.6 **Tracking Technologies**. Customer acknowledges that in connection with the performance of the Services, MailChimp employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("**Tracking Technologies**"). Customer shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable MailChimp to deploy Tracking Technologies lawfully on, and collect data from, the devices of Subscribers (defined below) in accordance with and as described in theMailChimp Cookie Statement.

5. Subprocessing

5.1 **Authorized Sub-processors**. Customer agrees that MailChimp may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by MailChimp and authorized by Customer are listed in **Annex A**.

5.2 **Sub-processor Obligations**. MailChimp shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause MailChimp to breach any of its obligations under this DPA.

6. Security

6.1 **Security Measures**. MailChimp shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with MailChimp's security standards described in **Annex B** ("**Security Measures**").

6.2 **Updates to Security Measures**. Customer is responsible for reviewing the information made available by MailChimp relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that MailChimp may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

6.3 **Customer Responsibilities**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

7. Security Reports and Audits

7.1 Customer acknowledges that MailChimp is regularly audited against SSAE 16 and PCI standards by independent third party auditors and internal auditors, respectively. Upon request, MailChimp shall supply (on a confidential basis) a summary copy of its audit report(s) ("**Report**") to Customer, so that Customer can verify MailChimp's compliance with the audit standards against which it has been assessed, and this DPA.
7.2 MailChimp shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm MailChimp's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

8. International Transfers

8.1 **Data center locations**. MailChimp may transfer and process Customer Data anywhere in the world where MailChimp, its Affiliates or its Sub-processors maintain data processing operations. MailChimp shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.
8.2 **Privacy Shield**. To the extent that MailChimp processes any Customer Data protected by EU Data Protection Law under the Agreement and/or that originates from the EEA, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that MailChimp shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data by virtue of having self-certified its compliance with Privacy Shield. MailChimp agrees to protect such Personal Data in accordance with the requirements of the Privacy Shield Principles. If MailChimp is unable to comply with this requirement, MailChimp shall inform Customer.
8.3 **Alternative Transfer Mechanism**. The parties agree that the data export solution identified in Section 8.2 shall not apply if and to the extent that MailChimp adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under EU Data Protection Laws) outside of the EEA ("**Alternative Transfer Mechanism**"), in which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Personal Data is transferred).

Part B: GDPR Obligations from 25 May 2018

9. Additional Security

9.1 **Confidentiality of processing**. MailChimp shall ensure that any person who is authorized by MailChimp to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).
9.2 **Security Incident Response**. Upon becoming aware of a Security Incident, MailChimp shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

10. Changes to Sub-processors

10.1 MailChimp shall (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which email shall suffice) if it adds or removes Sub-processors at least 10 days prior to any such changes.
10.2 Customer may object in writing to MailChimp's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

11. Return or Deletion of Data

11.1 Upon termination or expiration of the Agreement, MailChimp shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, save that this requirement shall not apply to the extent MailChimp is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data MailChimp shall securely isolate and protect from any further processing, except to the extent required by applicable law.

12. Cooperation

12.1 The Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, MailChimp shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to MailChimp, MailChimp shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If MailChimp is required to respond to such a request, MailChimp shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.
12.2 If a law enforcement agency sends MailChimp a demand for Customer Data (for example, through a subpoena or court order), MailChimp shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, MailChimp may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then MailChimp shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless MailChimp is legally prohibited from doing so.
12.3 To the extent MailChimp is required under EU Data Protection Law, MailChimp shall (at Customer's expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative:

The Rocket Science Group LLC d/b/a MailChimp

By:

Name: Daniel Kurzius
Title: CCO/Co-founder
Date: May 19, 2018

ODIK

Name: Rick Borkent
Title: Voorzitter
Date: May 19, 2018

Annex A - List of MailChimp Sub-processors

MailChimp uses its Affiliates and a range of third party Sub-processors to assist it in providing the Services (as described in the Agreement). These Sub-processors set out below provide cloud hosting and storage services; content delivery and review services; assist in providing customer support; as well as incident tracking, response, diagnosis and resolution services.

Entity Name	Corporate Location
Akamai	Massachusetts, USA
Amazon	Washington, USA
E-Hawk	New York, USA
El Camino	California, USA
FullContact	Colorado, USA
Google	California, USA
Neustar	Virginia, USA
R.R. Donnelley	Illinois, USA
Slack	California, USA
TaskUs	California, USA
Zendesk	California, USA

Annex B – Security Measures

The Security Measures applicable to the Services are described here https://mailchimp.com/about/security/ (as updated from time to time in accordance with Section 6.2 of this DPA).