Gegegevensverwerkersovereenkomst voor het verwerken van data in overeenstemming met de Duitse Federale Databeschermingswet (BDSG) en de EU Algemene Databescherming Richtlijn (EU GDPR)

tussen

Felyx E-scooters 1 BV
Herengracht 493
1017BT Amsterdam, Nederland

-hierna bekend als de Cliënt-

En

Fleetbird GmbH
Hansastrasse 95
44137 Dortmund, Duitsland

-hierna bekend als de Verwerker-

1. Onderwerp en duur van de overeenkomst
   1.1. Het onderwerp van deze overeenkomst vloeit voort uit het "DE_Softwarevertrag/DE_Softwareverdrag" of de "Software license agreement/Software licentie overeenkomst" (hierna: hoofdovereenkomst).
   1.2. De duur van deze overeenkomst is afhankelijk van de duur van de hoofdovereenkomst, zoals hierboven genoemd.

2. Verduidelijking van de contractuele inhoud
   2.1. De reikwijdte, aard en doel van het verzamelen, verwerken of gebruik van persoonsgegeven door de Verwerker voor de Cliënt kan als volgt worden omschreven: persoonsgegevens zullen worden verwerkt om een soepele operatie van de vloot deelvoertuigen te verzorgen. Op deze manier kunnen ritten, facturen en andere klantactiviteiten worden herhaald en gebruikt voor verdere verwerking.
   2.2. De contractueel overeengekomen dataverwerking zal enkel plaatsvinden in een lidstaat van de Europese Unie, of in een andere staat die is aangesloten bij het Verdrag inzake de Europese Economische Ruimte. Elke overdracht van data aan een derde land vereist de voorafgaande toestemming van de Cliënt en mag alleen plaatsvinden als aan de speciale vereisten voortvloeiend uit artikel 44 et seq. GDPR kunnen worden voldaan.
   2.3. De volgende types persoonsgegevens zullen worden verwerkt: persoonlijke mastergegevens, communicatiegegevens (bijvoorbeeld telefoonnummer, e-mailadres), contractuele mastergegevens (tarieven, contractuele relaties, producten of contruactele interesses), klantgeschiedenis, rijbewijsinformatie, contractuele betaalgegevens, planning en controlgegevens, informatie (van derde partijen, bijvoorbeeld kredietorganisaties of uit publieke bestanden).
   2.4. De categorieën personen betrokken bij de verwerking van deze gegevens zijn: klanten, werknemers, contacten, leveranciers.

3. Technische en organisatorische maatregelen

3.1. De Verwerker zal de implementatie van technische en organisatorische maatregelen vastleggen voorafgaand aan het plaatsen van een bestelling en het starten met verwerken, in het bijzonder in verband met de uitvoering van de bestelling en zal deze aan de Cliënt voorleggen ter controle. Na acceptatie van de Cliënt, zullen de vastgelegde en overeengekomen maatregelen de basis vormen voor deze overeenkomst. Als de controle/audit vanuit de Cliënt resulteert in de noodzaak voor aanpassing, zal dit met wederzijdse toestemming moeten worden geimplementeerd.

3.2. De Verwerker moet de beveiliging leveren krachtens paragraaf 9 BDSG en Art. 28 para. 3 lit. c, Art 32 GDPR, in het bijzonder in samenspel met art. 5 para. 1 para. 2 GDPR. In het algemeen zijn de maatregelen die moeten worden genomen databeschermingsmaatregelen, die genomen worden om een bepaald niveau van bescherming te bewerkstelligen, in verhouding tot het risico in verband met vertrouwelijkheid, integriteit, beschikbaarheid en weerbaarheid van de systemen. In dit verband moeten de geavanceerdheid, implentatiekosten, aard, reikwijdte en verwerkingsdoelen, en de wisselende waarschijnlijkheid en ernst van de te lopen risico's voor de rechten en vrijheden van de natuurlijke personen in de zin van Art. 32 (1) 1 GDPR worden betrokken (zie Bijlage).

3.3. Technische en organisatorische maatregelen zijn onderworpen aan technische vooruitgang en toekomstige ontwikkelingen. In dit verband is het de Verwerker toegestaan om adequate alternatieve maatregelen te implementeren. Het beveiligingsniveau van deze specifieke maatregelen moet adequaat zijn. Significante veranderingen moeten worden vastgelegd.

4. Aanpassing, restricties en verwijdering van data

4.1. De Verwerker mag op eigen gelegenheid het verwerken van de data van de Cliënt die ten behoeve van de Cliënt wordt verwerkt niet aanpassen, wissen of beperken, maar enkel in overeenstemming met vastgelegde instructies van de Cliënt. Als een betrokken persoon de Verwerker in dit verband benadert, zal de Verwerker onmiddellijk dit verzoek doorgeleiden naar de Cliënt.

4.2. Voor zover de reikwijdte van de dienstverlening ook, het verwijderingsconcept, het recht om te worden vergeten, aanpassing, data-overdracht en informatie betreft zal dit direct door de Verwerker worden afgehandeld, in overeenstemming met vastgelegde instructies van de Cliënt.

5. Controles, kwaliteitsgarantie en andere verplichtingen van de Verwerker

De Verwerker heeft additionele juridische verplichtingen voortvloeiend uit Art. 28 tot 33 GDPR om te handelen in overeenstemming met deze overeenkomst. In dit verband garandeert hij specifieke overeenstemming met de volgende vereisten:

5.1 Schriftelijke aanwijzing – voor zover vereist door de wet – van een functionaris voor gegevensbescherming die zijn/haar taken zal uitoefenen in overeenstemming met paragraven 4f, 4g BDSG of Art. 38 en Art. 39 Federale Databeschermingswet.

5.2 Om vertrouwelijkheid in overeenstemming met paragraaf 5 Federale Databeschermingswet en Art. 28 para. 3 lit. b, Art. 29, Art. 32 para. 4 GDPR te garanderen, zal de Verwerker enkel gebruik maken van medewerkers die gebonden zijn aan vertrouwelijkheid, en die zich eerder bekend hebben gemaakt met de relevante databeschermingsvoorschriften. De Verwerker en elk persoon onder zijn of haar beheer die toegang heeft tot persoonsgegevens mag deze data enkel verwerken in overeenstemming met de instructies van de Cliënt, inclusief de mogelijkheden toegewezen in deze overeenkomst, tenzij zij wettelijk verplicht zijn de voorgenomen verwerking uit te voeren.

5.3 De implementatie en inachtneming van alle technische en organisatorische maatregelen noodzakelijk voor de overeenkomst in overeenstemming met paragraaf 9 Federale Databeschermingswet of Art. 32 GDPR.
5.4 Op verzoek zullen de Cliënt en de Verwerker samenwerken met het relevante toezichtsorgaan voor wat betreft de uitoefening van hun taken en zij zullen elkaar hier onverwijld melding van doen. Dit geldt ook voor onderzoeken binnen het domein van administratieve overtredingen of strafrechtelijke processen, net als aansprakelijkheidsclaims van betrokken personen of derden, of andere claims verbonden aan de uitvoering van deze overeenkomst.
5.5 De Verwerker zal regulier interne processen en technische en organisatorische maatregelen monitoren om zeker te zijn dat het verwerken van data binnen zijn verantwoordelijkheid wordt uitgevoerd in overeenstemming met de vereisten van de toepasselijke databeschermingswetgeving en dat de rechten van de betrokkenen zijn beschermd.
5.6 Verifieerbaarheid van de technische en organisatorische maatregelen genomen vis-a-vis de Cliënt binnen de reikwijdte van zijn autoriteit in overeenstemming met paragraaf 7 van deze overeenkomst.

6. Relaties met onderaannemers
   6.1. Relaties met onderaannemers binnen het domein en betekenis van deze voorschriften zullen betekenen alle diensten die direct gelieerd zijn aan de voorschriften van de hoofddienstverlening. Dit betreft niet ondergeschikte diensten die de Verwerker gebruikt, waaronder telecommunicatie diensten, post/transport diensten, onderhoud en gebruikersdiensten of het opruimen van datahouders en andere maatregelen om vertrouwelijkheid, beschikbaarheid, integriteit en weerbaarheid van hardware en software of dataverwerkingssystemen te waarborgen. Echter, de Verwerker zal worden verplicht om noodzakelijke en wettelijke bindende contractuele overeenkomsten en controlemechanismen in te stellen om databescherming en dataveiligheid van de data van de Cliënt te beschermen, inclusief in het geval van uitbestede ondergeschikte diensten.
   6.2. De Verwerker mag alleen onderaannemers contracteren (andere verwerkers) met vooraf gegeven schriftelijke of anderszins vastgelegde toestemming van de Cliënt.
      De Cliënt gaat akkoord met de aanwijzing van de volgende onderaannemers op voorwaarde van een contractuele overeenkomst in overeenstemming met Art. 28 para. 2-4 GDPR:
      1. Amazon Web Services, Inc.: 410 Terry Ave North ; Seattle , WA 98109-5210, USA
         a. Server location: Frankfurt (EU)

      Het uitbesteden aan onderaannemers of het veranderen van bestaande onderaannemer is toegestaan, voorzover:
      a. De Verwerker de Cliënt vantevoren van dergelijke uitbesteding schriftelijk informeert en
      b. De Cliënt niet schriftelijk bezwaar maakt tegen deze voorgenomen uitbesteding tot het moment van overdracht van data aan de Verwerker en
      c. Een contractuele overeenkomst in overeenstemming met Art. 28 para. 2-4 GDPR als basis wordt gebruikt.

   6.3 De overdracht van de data van de Cliënt aan de onderaannemer en aanvang van zijn initiele activiteiten is alleen toegestaan als aan alle vereisten voor onderaanneming ziijn voldaan.
   6.4 Als de onderaannemer de overeengekomen diensten uitvoert buiten de EU/EER, zal de Verwerker afdoende maatregelen nemen om zeker te stellen dat dit is toegestaan onder de

de relevante wetten met betrekking tot databescherming. Hetzelfde geldt als dienstverleners worden gebruikt in overeenstemming met para. 1 zin 2.

6.5 Elke andere uitbesteding door de onderaannemer vereist de uitdrukkelijke toestemming van de hoofd cliënt (tenminste op schrift).

7. Controlerechten van de Cliënt

7.1. De Cliënt heeft het recht om inspecties uit te voeren in overleg met de Verwerker of deze te laten uitvoeren door inspecteur die in individuele zaken zijn aan te wijzen. Hij heeft het recht om periodieke willekeurige controles uit te voeren, welke als regel, ruim vantevoren moeten worden aangekondigd, in overeenstemming met deze overeenkomst door de Verwerker in zijn zakelijke dienstverlening.

7.2. De Verwerker zal ervoor zorg dragen dat de Cliënt niet verplicht is om te voldoen aan de verplichtingen van de Verwerker voortvloeiend uit paragraaf 11 para. 2 zin 4 Federale Databeschermingswet of Art. 28 GDPR. De Verwerker is verplicht om de noodzakelijke informatie op verzoek aan de Cliënt te doen toekomen en om in het bijzonder de implementatie van de noodzakelijke technische en organisatorische maatregelen aan te tonen.

7.3. Bewijs van zulke maatregelen, die niet alleen deze specifieke overeenkomst betreffen, kan worden geleverd door:

a. Naleving van goedgekeurde gedragsregels zoals beschreven in Art. 40 GDPR
b. Certificering door een goedgekeurde certificeringsprocedure in overeenstemming met Art. 42 GDPR
c. Huidige certificaten, verslagen of uittreksels van verslagen van onafhankelijke instanties (bijv auditors, review, functionarissen voor de gegevensbescherming, IT veiligheidsafdelingen, databeschermingsauditors, kwaliteitsauditors)
d. Toepasselijke certificering door een IT-veiligheid of dataveiligheidsaudit (bijvoorbeeld in overeenstemming met BSI-basis bescherming)

7.4. De Verwerker kan een claim voor een vergoeding bij de Cliënt indienen voor het uitvoeren van de inspecties.

8. Communicatie in het geval van overtredingen door de Verwerker

8.1. De Verwerker zal de Cliënt ondersteunen om te voldoen aan de verplichtingen gespecifieerd in paragraaf 42a Federale Databeschermingswet en artikelen 32 tot 36 GDPR op het gebied van veiligheid van persoonsgegevens, kennisgevingsverplichtingen in het geval van datalekken, data protection impact assessments en eerdere consultaties. Deze bevatten, maar zijn niet beperkt tot:

a. Zorgdragen voor een adequaat beschermingsniveau door middel van technische en organisatorische maatregelen, die de omstandigheden en doelen van de verwerking in acht nemen, samen met de voorspelde waarschijnlijkheid en ernst van een mogelijke inbreuk wegens kwetsbaarheden en die een onmiddellijke identificatie van de relevante overtredingen mogelijk maken
b. De verplichting om inbreuk op persoonsgegevens van de Cliënt zonder vertraging te rapporteren
c. De verplichting om de Cliënt te ondersteunen in de context van zijn verantwoordelijkheid om de betrokken persoon te informeren en om alle beschikbare informatie in dit verband aan hem zonder vertraging ter beschikking te stellen
d. Het ondersteunen van de Cliënt in de uitvoering van zijn data protection impact assessment

e. Het ondersteunen van de Cliënt in eerdere overleggen met de betrokken toezichthouder

8.2. De Verwerker is gerechtigd om een vergoeding te vragen voor ondersteunende diensten die niet in de dienstverleningsovereenkomst zijn gespecifieerd of die te wijten zijn aan ongepast gedrag van de Verwerker.

9. Autoriteit van de Cliënt om instructies uit te vaardigen

9.1. De Cliënt bevestigd mondelinge instructies zonder vertraging (tenminste op schriftelijke wijze).

9.2. De Verwerker moet de Cliënt onmiddellijk informeren als hij van mening is dat een instructie een overtreding betekent van databeschermingswetgeving. De Verwerker is geautoriseerd om de implementatie van deze instructie op te schorten tot deze is bevestigd of aangepast door personeel van de Cliënt.

10. Verwijdering en retour van persoonsgegevens

10.1 Kopieën of duplicaten van data mogen niet worden gecreerd zonder wetenschap van de Cliënt. Dit is exclusief back-ups, als die noodzakelijk zijn voor de uitvoering van een fatsoenlijke dataverwerking, of als deze noodzakelijk zijn om te voldoen aan de wettelijke dataretentieverplichtingen.

10.2 Bij voltooiing van het overeengekomen werk of eerder, op verzoek van de Cliënt - maar niet later dan bij beëindiging van de Dienstverleningsovereenkomst – zal de Verwerker alle documenten overhandigen die hij in zijn bezit heeft gekregen, concept verwerkings- of gebruikersgegevens, of deze vernietigen in lijn met databeschermingswetgeving, met vooraf gegeven toestemming. Hetzelfde geldt voor test en overtollig materiaal. Het logboek van de verwijdering moet op verzoek worden ingediend.

10.3 Documentatie die dient als bewijs van overeenkomst-overeenstemming en afdoende dataverwerking moeten door de Verwerker worden bewaard in overeenstemming met de toepasselijke bewaartermijnen na de termijn van deze Overeenkomst. Echter, voor zijn eigen gemak, mag de Verwerker ze ook terugsturen aan de Cliënt aan het einde van de looptijd van de Overeenkomst.

Voor de Verwerker:		Voor de Cliënt: Felyx E-scooters 1 BV	
Plaats, datum	Dortmund 25.05.18	Plaats, datum	Amsterdam 25 – 5 - 2018
Naam	10.2.e	Naam	10.2.e
Functie	COO Fleetbird	Functie	Co-founder
Handtekening	Geldige handtekening	Handtekening	Geldige handtekening

Bijlage: Technische en organisatorische maatregelen genomen door de Verwerker

In overeenstemming met paragraaf 9 Federale Databeschermingswet of Art. 32 GDPR (No. 3 van de privacy overeenkomst)

1. Vertrouwelijkheid (Art. 32 para. 1 letter b GDPR)

1.1 Toegangscontrole
Een ongeoorloofde toegang moet worden tegengaan waar de term ruimtelijk moet worden geinterpreteerd.

- Toegangscontrolesysteem: RFID chip
- Vastgelegde toewijzing van sleutels
- Toewijzing van sleutels/toegang enkel voor full/part-time/onderzoeksassistenten
- Deurveiligheid (elektrische deuropener, etc.)
- Ruimtes afsluiten aan het einde van de werkdag
- Gasten worden altijd begeleid en verwelkomt in het kantoorgebouw
- Toegangscontrole door geautoriseerde personen (bijv door personeel van de co-working ruimte)
- Surveillance uitrusting: alarmsysteem, cameratoezicht (niet in de kantoren), bewegingssensoren

1.2 Toegangscontrole
De toegang van ongeautoriseerde personen in de IT-systemen moet worden voorkomen.

- Servers kunnen alleen na een individuele login worden gebruikt
- Clients kunnen alleen na een individuele login worden gebruikt
- Login met wachtwoordbescherming (inclusief speciale karakters, minimale lengte)
- Automatische blokkering gedurende pauzes, IP spam en onjuiste loginpogingen (bijvoorbeeld wachtwoord of pauze wisselingen)
- Installatie van een gebruiker master logboek per gebruiker
- Standaard procedures voor het regulier updaten van beschermingssoftware
- Versleuteling van data houders

1.3 Toegangscontrole
Ongeautoriseerde activiteiten in IT-systemen buiten toegewezen rechten moet worden voorkomen.

- Er is een autorisatieprocedure met verschillende rechten (profielen, rollen, transacties en voorwerpen)
- Vrijgave/goedkeuring procedure gedefinieerd voor het toewijzen van goedkeuringen
- Aantal systeembeheerders sterk verminderd (kan door de Cliënt worden veranderd)
- Gebruik van veilige verwijderingsmethoden
- Loggen van informatie, veranderingen, verwijdering van data
- Evaluatie mogelijkheden

1.3 Gescheiden beheer
Data verzameld voor verschillende doelen moet ook apart worden verwerkt.

- Interne multi-client mogelijkheid (bijv data van verschillende klanten is logisch/fysiek gescheiden)
- Functionele scheiding (productie/test)

- Gebieden van competentie en verantwoordelijkheid zijn helder omschreven

1.4 Gebruik van pseudoniemen (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)
Een persoonlijke verwijzing is alleen mogelijk als aanvullende informatie kan worden toegevoegd.

- Persoonsgegevens worden alleen bewaard onder een pseudoniem (bijv een referentie-ID), voor zover dit mogelijk is gedurende het verwerken of overdracht aan systemen van derde partijen.
- De aanvullende informatie op basis waarvan een persoonlijke verwijzing kan worden gemaakt wordt versleuteld bewaard.

2. Integriteit (Art. 32 para. 1 letter b GDPR)

2.1 Controle op vrijgave
Bepaalde aspecten van het vrijgeven van persoonsgegevens moeten worden gereguleerd: elektronische verzending, data verzending, verzendingscontrole

- Versleutelde lijnen (SSL etc.)
- Loggen
- Versturen van met een wachtwoord beveiligde bestanden via e-mail

2.2 Controle op input
Traceerbaarheid en documentatie van datamanagement en onderhoud moeten worden verzekerd.

- Loggen en loganalyses
- Traceerbaarheid van input, aanpassing, en verwijdering van data door individuele gebruikersnamen (geen gebruikersgroepen)
- Controledata worden bewaard

3. Beschikbaarheid en afhankelijkheid (Art. 32 para. 1 letter b GDPR)

3.1 Controle van beschikbaarheid
De data moet worden beschermd tegen onbedoelde vernietiging of verlies. Hier moet je verwijzen naar de hosts en hun dienstverlening (aws.amazon.com)

- Backup en herstelprocedures
- Kopieren/spiegelen van harde schijven, bijv. RAID methodieken
- Gebruik van ononderbreekbare stroomtoevoer (UPS)
- Aparte/rampenvrije opslag van backups
- Gebruik van beschermingsprogramma's (virusscanners, firewalls, versleutelingsprogramma's, spam filets), noodplan is beschikbaar.

4. Procedure voor periodieke review, assessment en evaluatie (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

4.1 Databeschermingsmanagement
Databeschermingsmanagement verwijst naar de periodieke review, assessment en evaluatie van risico's,technische en communicatieve processen, en andere bestellings/overeenkomstge-relateerde onderwerpen in relatie tot het verwerken van data.

Fleetbird heeft interne mechanismen ontworpen om fatsoenlijke databescherming te bewerkstelligen middels een tweewegs-systeem:

1. Over perioden van vier tot zes weken worden procedures en interne processen inclusief infrastructuur, logs (technische protocollen), opslagmethoden, toegangsrechten, etc., besproken in teamoverleggen, onderzocht voor tijdigheid en veiligheid en in geval van twijfel worden maatregelen om de situatie te verbeteren overeengekomen.
2. Huidige systemen worden gecontroleerd door "real time" monitoring, in het bijzonder met betrekking tot beschikbaarheid, fouten, gedeeltelijke logging, etc. Op deze manier, kunnen individuen op korte termijn worden geinformeerd in het geval van problemen en kunnen contramaatregelen worden genomen.

4.2 Reactie en afhandeling van incidenten

Er is geen bijzondere procedure opgesteld, aangezien die onderdeel is van het normale werkproces. In het geval van databeschermingsincidenten, is dit de topprioriteit van het management en zal de Verwerker onmiddellijk worden geinformeerd en tegenmaatregelen worden genomen.

4.3 Standaard privacy instellingen (Art. 25 para. 2 GDPR)

Standaard en door toepasselijke technische en organisatorische maatregelen, zal worden verzekerd dat alleen persoonsgegevens die noodzakelijk zijn voor het betrokken verwerkingsproces worden verwerkt.

4.4 Controle van bestellingen

Verzekerd moet worden dat dataverwerking alleen plaatsvindt in overeenstemming met de gegeven instructies.

- Ondubbelzinnige opstelling van contracten
- Geformaliseerde plaatsing van bestellingen (bestellingsformulier)
- Criteria voor het vaststellen van de Verwerker
- Controle bij uitvoering van overeenkomsten