VERWERKERSOVEREENKOMST

De ondergetekenden:
MOOI Schoonheidsverzorging met ondernemingsnummer BE0840.465.705, hier rechtsgeldig

vertegenwoordigd door Karolien Piskor, verder genoemd klant (of verwerkingsverantwoordelijke)

Leverancier iBeauty BVBA, ondernemingsnummer **BE0662.785.756**, hier rechtsgeldig vertegenwoordigd door **Michel Smekens**, verder genoemd leverancier (of verwerker)

Overwegende dat:
De verwerkingsverantwoordelijke (klant) beschikt over persoonsgegevens, waarvan hij de verwerking wil toevertrouwen aan de verwerker (leverancier). Deze overeenkomst strekt ertoe om de uitvoering en de organisatie van die verwerking door de verwerker, te regelen en voldoende waarborgen te bieden ten aanzien van de bescherming van de persoonlijke levenssfeer.

Meer bepaald gaat het over de technische en organisatorische maatregelen – zoals vermeld in art. 32 van de Algemene Verordening Gegevensbescherming / General Data Protection Regulation (AVG/GDPR) - die tot doel hebben dat de verwerking voldoet aan de vereisten van de verordening en dat de bescherming van de rechten van de betrokkene is gewaarborgd. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

Artikel 1: Voorwerp van de overeenkomst (art. 28, lid 3, a)
De verwerker handelt uitsluitend in opdracht op basis van schriftelijke instructies, van de verwerkingsverantwoordelijke. Deze bepaling wordt letterlijk opgelegd door artikel 28, lid 3 van de AVG. Overeenkomstig de instructies van de verwerkingsverantwoordelijke en de bepalingen van deze overeenkomst zal de verwerker ten behoeve van de verwerkingsverantwoordelijke enkel persoonsgegevens verwerken volgens de bepalingen, zoals beschreven in bijlage 1.

Artikel 2: Naleving van de Algemene Verordening Gegevensbescherming
Partijen verbinden er zich principieel en uitdrukkelijk toe om de bepalingen van de Europese Verordening 2016/679 betreffende de bescherming van de natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens na te leven.

Artikel 3: Terbeschikkingstelling van de gegevens
Om de verwerker toe te laten de persoonsgegevens te verwerken, moeten die gegevens hem op de één of andere manier ter beschikking worden gesteld. Enkel de persoonsgegevens die strikt noodzakelijk zijn voor de doeleinden omschreven in artikel 1 mogen en kunnen door de verwerker worden verwerkt. De verwerking van de betreffende gegevens, alsmede de wijze van terbeschikkingstelling dienen steeds op een veilige manier te gebeuren.

Artikel 4: Gebruik van de persoonsgegevens (art. 28, lid 3, 4)
De gegevens mogen door de verwerker enkel worden verwerkt voor de doeleinden omschreven in bijlage 1 van deze overeenkomst. Dit houdt de principiële verplichting in om de gegevens enkel intern te gebruiken. De mededeling ervan aan derden, op welke wijze ook (door middel van doorzending, verspreiding of op enigerlei andere wijze) is verboden, tenzij dit door of krachtens een wet wordt opgelegd. Beroep doen op onderaannemers is ook een mededeling aan derden. Elke wettelijk verplichte mededeling van de persoonsgegevens, die het voorwerp zijn van deze overeenkomst, aan derden moet door de verwerker, indien mogelijk vooraf, ter kennis worden gebracht van de verantwoordelijke voor de verwerking.

Het is de verwerker verboden om van de ter beschikking gestelde gegevens een kopie te maken, behoudens met het oog op een back-up, indien dit noodzakelijk is bij het uitvoeren van de opdracht zoals omschreven in deze overeenkomst. De verwerker zal de gegevens niet langer bewaren dan noodzakelijk is voor het verrichten van de dienst waarvoor ze ter beschikking worden gesteld. Zijn de gegevens hierna niet meer nodig, dan zal de verwerker ze vernietigen dan wel terugbezorgen aan de verwerkingsverantwoordelijke.

Artikel 5: Gebruik sub-verwerkers (art. 28 lid 4)
De verwerker neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken. Het is de verantwoordelijkheid van de eerste verwerker een verwerkersovereenkomst af te sluiten met de tweede (derde, …) verwerker met de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden. Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de eerste verwerker ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker.

Artikel 6: Beveiliging (art. 32)
De verwerkingsverantwoordelijke en de verwerker treffen beide passende technische en organisatorische maatregelen om een passen beveiligingsniveau te waarborgen. De verwerkingsverantwoordelijke ziet erop toe dat de verwerker alle vereiste maatregelen (zoals opgesomd in art. 32 van de AVG) neemt. Deze maatregelen worden beschreven in bijlage 2 bij deze overeenkomst.

In het bijzonder zal de verwerker de persoonsgegevens beveiligen tegen vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

De verwerker zal de verantwoordelijke voor de verwerking steeds informeren over de technische en organisatorische maatregelen die hij ten uitvoer heeft gelegd om de persoonsgegevens te beveiligen tegen vernietiging, verlies, vervalsing en niet-toegelaten verspreiding of toegang.

Artikel 7: Fysische toegangsbeperking
De verwerker zal ervoor zorgen dat de plaatsen waar ten behoeve van de verwerkingsverantwoordelijke voor de verwerking persoonsgegevens worden verwerkt, niet toegankelijk zijn voor onbevoegden. Daartoe zal hij onder meer de nodige organisatorische maatregelen nemen.

Artikel 8: Functionele toegangsbeperking
De verwerker zal de toegang tot de verwerkte persoonsgegevens beperken tot die personeelsleden die de gegevens nodig hebben om de taken uit te oefenen die de verwerker hen in uitvoering van deze overeenkomst toewijst. Daartoe zal de verwerker aan de verwerkingsverantwoordelijke een lijst bezorgen van de personeelsleden die betrokken zijn bij de verwerking te zijnen behoeve van persoonsgegevens.

Indien een opsomming van alle personeelsleden al te omslachtig is, kan geopteerd worden voor een opsomming van de diensten of afdelingen.

Artikel 9: Voorlichting (art. 29)
De verwerker verbindt er zich toe om de personen die overeenkomstig deze overeenkomst toegang hebben tot de gegevens, in kennis te stellen van de bepalingen van de Algemene Verordening Gegevensbescherming. De verwerker waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.

Artikel 10: Toepassing van de kennisgevingsplicht (art. 13)
Indien de verwerker in de uitvoering van deze overeenkomst, persoonsgegevens rechtstreeks verkrijgt bij de betrokkenen en deze gegevens registreert, zal hij de bepalingen van artikel 13 van de algemene gegevensverordening naleven en de betrokkenen informeren (middels bv een privacy beleid).

In voorkomend geval wordt overeengekomen dat de verwerker de inhoud en wijze van de kennisgeving vooraf aan de verwerkingsverantwoordelijke voorlegt.

Artikel 11: Controle door de verwerkingsverantwoordelijke (art. 28 lid 3, h)
De verwerkingsverantwoordelijke heeft op elk ogenblik het recht om de naleving van deze overeenkomst te controleren. Op eenvoudig verzoek van de verantwoordelijke is de verwerker ertoe gehouden alle informatie ter beschikking te stellen die nodig is om de nakoming van de neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk te maken en eraan bij te dragen.

Artikel 12: Aansprakelijkheid (art. 82, lid 2)
De verwerker is alleen en volledig aansprakelijk voor de schade die voortvloeit uit de niet-naleving van de bepalingen van deze overeenkomst en haar bijlagen. Indien de verwerkingsverantwoordelijke door een betrokkene wordt aangesproken in schadevergoeding, zal de verwerker, op eenvoudig verzoek van de verantwoordelijke, in de procedure tussenkomen teneinde de verwerkingsverantwoordelijke te vrijwaren.

Artikel 13: Verplichting na beëindiging van de verwerking van persoonsgegevens (art. 28, lid 3, g)
De partijen komen overeen dat de verwerker na beëindiging van de verlening van gegevensverwerkingsdiensten alle doorgegeven persoonsgegevens en kopieën daarvan aan de klant terugbezorgt of, indien de klant dit verkiest, alle persoonsgegevens vernietigt en aan de klant verklaart dat de vernietiging heeft plaatsgevonden, tenzij de op de verwerker toepasselijke wetgeving hem verbiedt alle of een gedeelte van de doorgegeven persoonsgegevens veilig terug te bezorgen of te vernietigen. In dat geval garandeert de leverancier dat hij de vertrouwelijkheid van de doorgegeven persoonsgegevens zal respecteren en dat hij de doorgegeven persoonsgegevens niet actief zal verwerken.

Leverancier Datum:

Klant Datum:

Leverancier Locatie:

Klant Locatie:

Bijlage 1: Doeleinden

Bijlage 2: Beschrijving van de technische en organisatorische maatregelen zoals beschreven in art. 32 AVG

Verwerkersovereenkomst – Bijlage 1

Onderwerp van de verwerking

Duur van de verwerking

Aard en doel van de verwerking

Soort persoonsgegevens die worden verwerkt

Categorieën van betrokkenen bij de verwerker

Verwerkersovereenkomst – Bijlage 2

Bepalingen art 32 AVG

Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen.

De verwerker is eraan gehouden om maatregelen te treffen die onder meer het volgende omvatten:
- de pseudonimisering en versleuteling van persoonsgegevens
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreff. endheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking. Hiertoe geeft de verwerking hieronder een opsomming van de toegepaste beveiligingsmaatregelen.

Beschrijving van de mogelijke technische en organisatorische maatregelen

1 Technische maatregelen

- De aanwezigheid van automatische anonimisering of pseudonimisering van de persoonsgegevens nadat het doeleinde van de verwerking (of wettelijke opgelegde bewaartermijnen) zijn overschreden
- De aanwezigheid van een degelijk uitgebouwd gebruikers beheer. Dit omvat:
  - Het bestuur moet zelf interne gebruikers kunnen toevoegen/verwijderen (zonder tussenkomst v/d leverancier)
  - De mogelijkheid om multi-factor authenticatie (bv. eID) te gebruiken
  - De mogelijkheid om een wachtwoordenpolicy in te stellen (gebruikers - burgers) kiezen zelf hun inloggegevens, deze worden niet in de back-end bepaald)
  - De mogelijkheid om het wachtwoord van een gebruiker te resetten
  - Minstens 2 niveau's van rechten (een administrator en gebruikers) naargelang gebruik- en beslissingsniveau
  - ...
- Een degelijk uitgebouwde audit log module
  - De mogelijkheid tot loggen van: welke gebruiker, welke acties in het programma heeft uitgevoerd (incl. consultatie).
  - Raadpleegbaar door de klant (het bestuur) zonder tussenkomst van de leverancier.
  - Logging van uitgevoerde tussenkomsten door de leverancier, raadpleegbaar door de klant zonder tussenkomst van de leverancier.
  - …
- Mogelijkheid tot extractie (export) van gegevens / back-up mogelijkheid

Daarnaast moet een webapplicatie beschikken over:
- Een grondige beveiliging uitgevoerd op basis van de OWASP top 10 bedreigingen
  - Met minstens een bescherming tegen een brute force aanval (mogelijkheid tot blokkeren van gebruikers na x aantal pogingen tot inloggen)
- Structurele bijwerkingen op het vlak van security:
  - Aan server (besturingssysteem, webserver, antivirus, …)
  - Aan databank
  - Aan gebruikt platform voor de webapplicatie

Enige overdracht en opslag van persoonsgegevens, vervat in de toepassing, dient op een veilige manier te gebeuren. Indien het om een webapplicatie gaat gelden volgende minimale vereisten:

- De persoonsgegevens worden via een beveiligde verbinding (https, VPN, IPSEC, FTPS) ter beschikking gesteld.
  - Een beveiligde verbinding voor eindgebruikers
  - Een beveiligde verbinding met het Rijksregister
- De persoonsgegevens worden opgeslagen in een Europees datacenter (liefst ISO27001 gecertificeerd)
- Een back-up van de persoonsgegevens wordt – indien van toepassing bvb bij het werken met een tweede datacenter – ook via een beveiligde verbinding doorgegeven. Daarnaast wordt de back-up procedure van de leverancier gedocumenteerd.
- Data opslag gebeurt versleuteld, minstens voor de wachtwoorden.

2 Organisatorische maatregelen

- De leverancier beschikt over een veiligheidsconsulent
- De leverancier toont aan dat zijn eventuele personeelsleden op de hoogte zijn van het veiligheidsbeleid
- De leverancier garandeert de klant d.m.v. afspraken dat de opgeslagen persoonsgegevens door de leverancier enkel worden ingekeken op vraag van de klant of na verwittiging voor onderhoud
- De leverancier toont aan via documentatie dat hij in staat is om bij een data-lek klanten te informeren
- Een privacyverklaring geeft de nodige transparantie (principe van privacywet)
- De leverancier garandeert in een SLA maximale onderbrekingen en een contactpunt bij incidenten.