Verwerkersovereenkomst CoBoo

Versie 1.0, laatst bijgewerkt 13 november 2026

Partijen

1. de organisatie die de diensten van CoBoo afneemt, hierna: Verwerkingsverantwoordelijke;
2. CoBoo, mede handelend onder de naam Lumyo, gevestigd te Hoogeveen, ingeschreven bij de Kamer van Koophandel onder nummer 99516551, vertegenwoordigd door Colin Suttner, hierna: Verwerker.

Partijen sluiten deze overeenkomst omdat Verwerker voor Verwerkingsverantwoordelijke phishing-simulaties uitvoert en toegang geeft tot de Lumyo awareness training (de Hoofdovereenkomst: de geaccepteerde offerte met de algemene voorwaarden van CoBoo). Daarbij verwerkt Verwerker persoonsgegevens van medewerkers van Verwerkingsverantwoordelijke.

Artikel 1. Begrippen

Begrippen als persoonsgegevens, verwerking, betrokkene, inbreuk in verband met persoonsgegevens (datalek) en subverwerker hebben de betekenis uit de Algemene Verordening Gegevensbescherming (AVG). Medewerkers zijn de personen die Verwerkingsverantwoordelijke aanmeldt voor een simulatie of training.

Artikel 2. Onderwerp en instructies

1. Verwerker verwerkt persoonsgegevens uitsluitend in opdracht en op schriftelijke instructie van Verwerkingsverantwoordelijke, en alleen voor de uitvoering van de Hoofdovereenkomst. De Hoofdovereenkomst en deze overeenkomst gelden samen als die instructie.
2. Verwerker gebruikt de persoonsgegevens niet voor eigen doeleinden. Geanonimiseerde totalen die niet tot een persoon of klant herleidbaar zijn, mag Verwerker gebruiken om de dienst te verbeteren.
3. Vindt Verwerker dat een instructie in strijd is met de AVG, dan meldt hij dat direct.
4. Welke gegevens, van wie, waarvoor en hoe lang staat in Bijlage 1.

Artikel 3. Doel en grondslag

1. Doel van de verwerking is het meten en verbeteren van de weerbaarheid van medewerkers tegen phishing, via gesimuleerde phishing-mails, rapportage en training.
2. Verwerkingsverantwoordelijke bepaalt de grondslag (in de regel een gerechtvaardigd belang), informeert de medewerkers vooraf in algemene zin over het programma, en stemt waar nodig af met de ondernemingsraad.
3. Resultaten worden standaard per afdeling gerapporteerd. Rapportage per medewerker vindt alleen plaats op uitdrukkelijk schriftelijk verzoek van Verwerkingsverantwoordelijke, die dan zelf verantwoordelijk is voor het zorgvuldige gebruik ervan. Resultaten worden niet gebruikt voor sancties tegen individuele medewerkers, tenzij Verwerkingsverantwoordelijke daar zelf een grondslag voor heeft.

Artikel 4. Verplichtingen van Verwerker

1. Verwerker verwerkt alleen de persoonsgegevens die voor de dienst nodig zijn (dataminimalisatie).
2. Wat een medewerker invult op een gesimuleerde inlog- of formulierpagina, wordt niet opgeslagen. Verwerker legt alleen vast dat er iets is ingevuld, nooit wachtwoorden of andere ingevulde waarden.
3. Verwerker helpt Verwerkingsverantwoordelijke, voor zover redelijk, bij een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging van de Autoriteit Persoonsgegevens.

Artikel 5. Geheimhouding

Iedereen die bij Verwerker toegang heeft tot de persoonsgegevens, is tot geheimhouding verplicht. Dat geldt niet als een wettelijke plicht tot verstrekking bestaat; Verwerker meldt zo'n verzoek dan vooraf aan Verwerkingsverantwoordelijke, tenzij de wet dat verbiedt.

Artikel 6. Beveiliging

1. Verwerker neemt passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking, rekening houdend met de stand van de techniek, de kosten en de risico's voor medewerkers.
2. De maatregelen staan in Bijlage 3. Verwerker mag ze aanpassen, zolang het beveiligingsniveau niet lager wordt.

Artikel 7. Subverwerkers

1. Verwerkingsverantwoordelijke geeft algemene toestemming voor de subverwerkers in Bijlage 2.
2. Een nieuwe of andere subverwerker meldt Verwerker minimaal 30 dagen vooraf. Verwerkingsverantwoordelijke kan binnen die termijn op redelijke gronden bezwaar maken; komen partijen er niet uit, dan mag Verwerkingsverantwoordelijke de Hoofdovereenkomst opzeggen voor het deel waar de subverwerker bij betrokken is.
3. Verwerker legt subverwerkers dezelfde verplichtingen op als in deze overeenkomst en blijft tegenover Verwerkingsverantwoordelijke verantwoordelijk voor hen.

Artikel 8. Datalekken

1. Verwerker meldt een datalek zonder onnodige vertraging en uiterlijk binnen 24 uur nadat hij het ontdekt aan de contactpersoon van Verwerkingsverantwoordelijke.
2. De melding bevat, voor zover bekend: wat er is gebeurd, welke gegevens en hoeveel medewerkers het betreft, de waarschijnlijke gevolgen en de genomen of voorgestelde maatregelen. Wat nog niet bekend is, volgt zodra het bekend is.
3. Verwerkingsverantwoordelijke beslist of het datalek wordt gemeld aan de Autoriteit Persoonsgegevens en aan medewerkers; Verwerker helpt daarbij.

Artikel 9. Rechten van medewerkers

Krijgt Verwerker een verzoek van een medewerker (zoals inzage, correctie of verwijdering), dan stuurt hij dat door aan Verwerkingsverantwoordelijke en handelt hij het niet zelf af. Verwerker helpt

Verwerkingsverantwoordelijke binnen redelijke termijn om zulke verzoeken te beantwoorden.

Artikel 10. Doorgifte buiten de EER

Verwerker slaat de persoonsgegevens op binnen de Europese Economische Ruimte. Doorgifte daarbuiten, ook door een subverwerker, gebeurt alleen met een geldige grondslag uit hoofdstuk V van de AVG, zoals een adequaatheidsbesluit of de standaardcontractbepalingen van de Europese Commissie.

Artikel 11. Controle (audit)

1. Verwerker geeft Verwerkingsverantwoordelijke op verzoek de informatie die nodig is om naleving van deze overeenkomst aan te tonen.
2. Verwerkingsverantwoordelijke mag maximaal eens per jaar, na aankondiging van minimaal 30 dagen, een controle laten uitvoeren door een onafhankelijke deskundige met geheimhoudingsplicht. De kosten zijn voor Verwerkingsverantwoordelijke, tenzij de controle laat zien dat Verwerker deze overeenkomst op wezenlijke punten niet nakomt.

Artikel 12. Duur, bewaren en verwijderen

1. Deze overeenkomst loopt zolang de Hoofdovereenkomst loopt, en daarna zolang Verwerker nog persoonsgegevens van Verwerkingsverantwoordelijke heeft.
2. Na afloop van de Hoofdovereenkomst bewaart Verwerker de persoonsgegevens, inclusief de resultaten per medewerker, nog maximaal 12 maanden, zodat de nulmeting, de trend en de grafieken, ook per medewerker, doorlopen als de klant binnen die periode terugkomt. Verwerkingsverantwoordelijke kan op elk moment vragen om eerdere verwijdering of om teruggave in een gangbaar bestandsformaat.
3. Na die termijn verwijdert Verwerker de persoonsgegevens, ook bij subverwerkers en uit back-ups zodra die worden overschreven, en bevestigt dat op verzoek schriftelijk. Geanonimiseerde totalen vallen hier niet onder.

Artikel 13. Aansprakelijkheid

1. Op de aansprakelijkheid van Verwerker onder deze overeenkomst is de regeling over aansprakelijkheid in de algemene voorwaarden van CoBoo van toepassing, inclusief het maximum per kalenderjaar dat daarin staat.
2. Dat maximum geldt voor alle aanspraken onder deze overeenkomst en de Hoofdovereenkomst samen; deze overeenkomst kent geen eigen of hoger maximum.
3. Verwerker is niet aansprakelijk voor schade of boetes die het gevolg zijn van een instructie van Verwerkingsverantwoordelijke, of van het niet nakomen door Verwerkingsverantwoordelijke van diens eigen verplichtingen uit de AVG, zoals het informeren van medewerkers.
4. Een boete die de Autoriteit Persoonsgegevens aan Verwerkingsverantwoordelijke oplegt, komt alleen voor rekening van Verwerker voor zover die boete rechtstreeks het gevolg is van een tekortkoming van Verwerker zelf, en binnen de grenzen van lid 1 en 2.
5. Deze beperkingen gelden niet bij opzet of bewuste roekeloosheid van Verwerker.

Artikel 14. Slotbepalingen

1. Bij strijd tussen deze overeenkomst en de Hoofdovereenkomst gaat deze overeenkomst voor, voor zover het de verwerking van persoonsgegevens betreft.
2. Wijzigingen gelden alleen nadat Verwerkingsverantwoordelijke ze heeft aanvaard zoals beschreven onder Aanvaarding.
3. Op deze overeenkomst is Nederlands recht van toepassing. Geschillen worden voorgelegd aan de bevoegde rechter in het arrondissement Noord-Nederland.

Aanvaarding

1. Deze overeenkomst komt tot stand doordat een bevoegde vertegenwoordiger van Verwerkingsverantwoordelijke haar elektronisch aanvaardt bij het aanmaken van het account, vóór de eerste verwerking. Partijen erkennen dat deze elektronische aanvaarding geldt als schriftelijke ondertekening (artikel 28 lid 9 AVG en artikel 6:227a Burgerlijk Wetboek).
2. Bij de aanvaarding legt Verwerker vast: naam en functie van de persoon die aanvaardt, de organisatie, de datum en het tijdstip, en de versie van deze overeenkomst. Verwerker neemt die gegevens op in het document en stuurt het per e-mail naar Verwerkingsverantwoordelijke. Dat gemailde document is de geldende overeenkomst.
3. Bij een wijziging ontvangt Verwerkingsverantwoordelijke een e-mail met de nieuwe versie, en aanvaardt die door in te loggen en opnieuw akkoord te geven. Tot dat moment blijft de vorige versie gelden. Wordt een wijziging niet binnen 30 dagen aanvaard, dan mogen beide partijen de Hoofdovereenkomst opzeggen.

Deze overeenkomst wordt aanvaard in het klantportaal; organisatie, naam en functie van de ondertekenaar en datum en tijdstip worden daarbij vastgelegd.

Versie: 1.0, 13 november 2026

Bijlage 1. Specificatie van de verwerking

Betrokkenen: medewerkers van Verwerkingsverantwoordelijke die aan een simulatie of training deelnemen. Bijzondere persoonsgegevens (zoals gezondheid) en het burgerservicenummer worden niet verwerkt.

Onderdeel	Persoonsgegevens	Waarvoor
Deelnemerslijst	Voor- en achternaam, e-mailadres, functie (optioneel), afdeling, vestiging of land, taal	Mails versturen in de juiste taal, uitsplitsing per afdeling of land
Phishing-simulatie	Per medewerker met datum en tijd: mail ontvangen, geopend, link aangeklikt, iets ingevuld (alleen dát, niet wat), mail gemeld	Weerbaarheid meten, nulmeting, hermeting en trend
Technische gegevens bij een klik	IP-adres, browser en besturingssysteem, globale locatie afgeleid uit het IP-adres	Echte klikken onderscheiden van automatische scans door mailservers
Lumyo awareness training	Account (inlognaam, versleuteld wachtwoord), gevolgde modules met datum, scores op kennistests, certificaten	Training geven, voortgang en certificaten bijhouden
Rapportage	Totalen per afdeling; per medewerker alleen op schriftelijk verzoek	Rapport aan Verwerkingsverantwoordelijke

Bewaartermijn: zolang de Hoofdovereenkomst loopt, en daarna maximaal 12 maanden (artikel 12).

Contactpersonen: Verwerkingsverantwoordelijke: de contactpersoon die de Verwerkingsverantwoordelijke bij aanvaarding opgeeft. Verwerker: CoBoo, contact@coboo.nl.

Bijlage 2. Subverwerkers

De phishing-software (Gophish) en het Lumyo-platform draaien op een eigen server van Verwerker in Nederland; daar is geen hostingpartij bij betrokken.

Subverwerker	Wat	Gegevens	Locatie
Mailgun (Sinch)	Versturen van de gesimuleerde phishing-mails	E-mailadres, naam, mailinhoud, afleverstatus	EU-regio (account op de EU-omgeving)

Mailgun bewaart de berichtgegevens van een domein in de EU-regio alleen in die regio. Mailgun hoort bij een Amerikaans concern (Mailgun Technologies, Inc., onderdeel van Sinch). Voor eventuele toegang vanuit de VS geldt de certificering van Mailgun Technologies, Inc. onder het EU-VS Data Privacy Framework; anders vallen doorgiften onder de standaardcontractbepalingen van de Europese Commissie. Grondslag en voorwaarden staan in de verwerkersovereenkomst van Sinch.

Bijlage 3. Beveiligingsmaatregelen

- Toegang: alleen Verwerker zelf heeft toegang tot de persoonsgegevens; er werken geen andere personen mee.
- Inloggen: tweestapsverificatie op alle beheeromgevingen: de server, Gophish, het Lumyo-platform en het Mailgun-account.
- Versleuteling: alle verbindingen via HTTPS (TLS); opslag en back-ups versleuteld.
- Back-ups: regelmatige back-ups, die na de bewaartermijn uit artikel 12 mee worden opgeruimd.
- Updates: besturingssysteem en software worden bijgehouden en beveiligingsupdates worden tijdig geïnstalleerd.

- Dataminimalisatie: ingevulde wachtwoorden en andere ingevulde waarden op simulatiepagina's worden nooit opgeslagen.
- Scheiding: gegevens van verschillende klanten worden gescheiden gehouden en alleen voor die klant gebruikt.